Troubleshooting

Chapter 1 Method of Local Initial Measures According to Maintenance Request ····· TRBL 01-0000

Chapter 2 Troubleshooting Flowchart ····· TRBL 02-0000

Chapter 3 Maintenance Procedure of Power Supply Failures ····· TRBL 03-0000

Chapter 4 Determination of Management Network Failure ····· TRBL 04-0000

Chapter 5 Method of Determining Failure Information ····· TRBL 05-0000

Chapter 6 Acquiring Failure Information ····· TRBL 06-0000

Chapter 7 Failure Monitoring by SNMP ····· TRBL 07-0000

Chapter 8 Messages ····· TRBL 08-0000

Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure ····· TRBL 09-0000

Chapter 10 Appendix A fsrepair Command ····· TRBL 10-0000

Chapter 11 Appendix B The Outline of the Troubleshooting Procedure ····· TRBL 11-0000

Chapter 12 Appendix C The Entire Restoration Procedures on HDI Side in the Configuration of HDI for Cloud ····· TRBL 12-0000

Copyright © 2010, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

Chapter 1 Method of Local Initial Measures According to Maintenance Request

The contents of local initial measures according to the maintenance request when a failure occurs in Hitachi Data Ingestor are described.

Note that if the target model is HA8000 Series, you must refer to "C.1 Local Initial Operations According to Maintenance Request" in advance.

For the Configuration of single node with spare for Cloud, read "Theory '3.2.2.1 Operation policy when a failure occurs in the single node configuration (3)' (THEO 03-0070)" first before executing the maintenance work. Basically, execute the failure recovery for the node isolated from the failure occurred front-end LAN.

1.1 Failure Detection by Hitachi Data Ingestor

NOTE: If the appearance of MAINTENANCE lamp of the target model is different from Figure 1.1-1, refer to Troubleshooting "1.5 Appendix Contents Indicated by MAINTENANCE Lamp of Each Model" (TRBL 01-0050) and read the indication and meaning of the MAINTENANCE lamp properly.

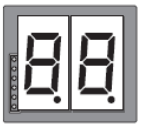


Figure 1.1-1 Appearance of MAINTENANCE Lamp

A failure in Hitachi Data Ingestor is detected by the following methods.

(1) Detected by HiTrack

(2) The system administrator notices the failure detected by SNMP Trap

(3) The system administrator notices the following failures visually
- Power supply unit, internal drive and others, LED lighting on parts
- Abnormal OS operation, abnormal environment
- Impossible to access the both nodes from the HFSM.
- The entire failure on the side of HDI in the configuration of HDI for Cloud environment (*1)
- Notice an abnormal occurrence such as an OS access impossible in the single node configuration.

*1: The entire failure on the side of HDI means the failure that requires the resetting all of the equipments (nodes, disk array, network devices, and environment servers etc.) from the initial state due to an occurrence such as a disaster on the HDI placed area.

(4) The maintenance personnel notice the failure by LED lighting, which is front of the node.
About the LED status, refer to Troubleshooting "1.5 Appendix Contents Indicated by MAINTENANCE Lamp of Each Model" (TRBL 01-0050).

Copyright © 2011, 2016, Hitachi, Ltd.

1.2 Maintenance Request and Method of Local Initial Measurement

The failure detected by HiTrack or the system administrator is notified to the Maintenance Center of (HDS) (maintenance request). As the local initial measures for this maintenance request, the maintenance personnel should collect the failure information at the time of failure notice.

The collection method of the failure information differs depending on the method of the failure detection.

NOTE:
- When executing OS termination (stopping auto power supply or stopping power supply by the power lamp switch, stopping by a command instruction), a part of failure information might be disappeared. Therefore, do not stop OS unless otherwise there is such instruction to stop the OS or there is a special instruction.
- Check whether the maintenance LAN IP-SW is owned by (HDS) or customer.
- When performing troubleshooting in the configuration where KVM is not used, read “KVM” in this manual as "Remote console."
- In the case of CR220SM, an external DVD-ROM drive is required for performing HATP. Ask the system administrator about external DVD-ROM drive because it is an accessory of the product. If there is no external DVD-ROM drive, the maintenance personnel must prepare it. For how to connect, refer to “A.2.1.2 External DVD-ROM drive.”
- When collecting Simple log by using HATP, select “3 (ALL escalation log)” in “Select menu number” of HATP menu (2) Log collect menu to collect a complete log.
  For details, refer to the maintenance manual of the target model (HA8000 series / CR2x0 series).
- HATP might be used for collecting logs or locating faulty hardware. If the node to be maintained is CR210HM or CR220SM, be sure to turn off the node before performing HATP. Make sure that the CD of HATP is not inserted before turning off the node, or the node cannot be restarted.

(1) When detected by HiTrack
Refer to “C.1.1 When Detected by HiTrack”.

(2) When detected by SNMP Trap
Refer to “C.1.2 When Detected by SNMP Trap”.

(3) When detected by the system administrator visually
Refer to “C.1.3 When the System Administrator Noticed a Failure”.
However, in the case of entire failure on HDI side in the configuration of HDI for Cloud environment, refer to Troubleshooting “1.4 Restoration Procedures for the Entire Failures on HDI Side at the Configuration of HDI for Cloud Environment” (TRBL 01-0040).

(4) When detected by the maintenance personnel (at the time of initial installation)
Refer to “C.1.4 When the Maintenance Personnel Noticed the Failure at the Time of Initial Installation in the Local Site”.

Copyright © 2012, 2015, Hitachi, Ltd.

1.3 This Page is Intentionally Blanked

Copyright © 2011, 2014, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, 2014, Hitachi, Ltd.

1.4 Restoration Procedures for the Entire Failures on HDI Side at the Configuration of HDI for Cloud Environment

In the configuration of HDI for Cloud, the setting on the side of HDI can be restored if the entire systems on the HDI side failed. Note that, in the single node configuration, the system administrator must execute data recovery after OS installation.
However, the following conditions must be met.

- In the cluster configuration, distributors must store the serial number of disk array subsystem per customer or site, and apply it when shipping a disk array subsystem for the restoration of HDI side.

- System Administrator must execute the following migration operation periodically (assumed 1 time/ day).

  User data: Every file systems of HDI must be set OS: “the entire file system makes the subject of migration”.

  System configuration information: Regular Backup of System configuration information to HCP must be performed.

- System administrator must store the following information of HDI side to the place where unaffected of HDI failure.
  - IP segment, IP address, and routing information of each Network equipment.
  - Setting of environment servers (interface setting of DNS) to make interface with HCP.
  - Configuration file that is recorded the setting of disk array. (In the cluster configuration)
  - Backup file that is recorded the sharing in formation of file system. (In the cluster configuration)
  - A combination of File system name and Namespace name. (In the cluster configuration)
  - Key codes for encryption of data stored on a HCP system (In the case that HCP payload encryption function is enabled).

- The system administrator of HCP side on a configuration of HDI for Cloud must store the following information per HDI to be connected.
  - Accessing account
  - Migration policy name
  - Tenant name/ System name
  - The place to be stored the system configuration information file.

    The following example shows when the host name of HCP to be stored is “hcp.hitachi.com”, the name space is NS1, and the tenant name is tenant1.

    (e.g.): http:// NS1.tenant1.hcp.hitachi.com/rest/system/system_backupfile.tgz

For the details of restoration procedure in the cluster configuration, refer to Troubleshooting “Chapter 12 Appendix C The Entire Restoration Procedures on HDI Side in the Configuration of HDI for Cloud” (TRBL 12-0000).

For the details of restoration procedure in the single node configuration, refer to Troubleshooting “9.2.3.1.1 Failure recovery of the blocked file system in the Configuration using Management port when not connected to the disk array subsystem” (TRBL 09-0720) in case of a failure in the Configuration using Management port and Troubleshooting “9.2.3.1.2 Failure recovery of the blocked file system in the Configuration using trunk 2 Data ports when not connected to the disk array subsystem” (TRBL 09-0730) in case of a failure in the Configuration using trunk 2 Data ports.

Copyright © 2011, 2015, Hitachi, Ltd.

1.5 Appendix Contents Indicated by MAINTENANCE Lamp of Each Model

NOTE: D51B-2U does not have a LED corresponding to MAINTENANCE Lamp. To specify the failure part, log into MegaRAC GUI and check Event Log. For the details of MegaRAC GUI, refer to “QuantaGrid Series D51B-2U Technical Guide”.

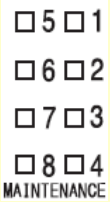
MAINTENANCE lamp indicates system operating status.

There are three types of system operating status to be indicated: event code, POST code, and power consumption, which can be switched by SERVICE lamp switch. For the details about how to switch the system operating status to be indicated, refer to the maintenance manual of the target model (HA8000 series / CR2x0 series).

When event code is the system operating status currently indicated, the lamp indication means the part where an error occurred. However, the shape of MAINTENANCE lamp differs depending on the model. Therefore indication also differs by model.

Table 1.5-1 shows the indication of MAINTENANCE Lamp of Each Model, and meanings of the indication.

Table 1.5-1 Contents Indicated by MAINTENANCE Lamp of Each Model

Shapes and indications of MAINTENANCE lamp			Error occurrence part
1	2	3	
			
LED 1 on		80 on	CPU
LED 2 on		40 on	Memory
LED 3 on		20 on	Mother board
LED 4 on		10 on	PCI
LED 5 on		08 on	Power supply/Voltage
LED 6 on		04 on	Fan
LED 7 on		02 on	Temperature
LED 8 on		01 on	Other hardware
All lamps off		00 on	No error (power-on status)
		All lamps off	No error (power-off status)

All MAINTENANCE Lamps above (1 to 3) indicate the error status.
For example, on the occurrence of a temperature anomaly, LED 7 lights up on MAINTENANCE lamp 1 and 2 while “02” is displayed on MAINTENANCE lamp 2.
Also, on the occurrence of HDD error and temperature anomaly, LED 7 and LED 8 light up on MAINTENANCE lamp 1 and 2 while “03”, which is the sum of “01” and “02” in hexadecimal, is displayed on MAINTENANCE lamp 2.

Copyright © 2011, 2016, Hitachi, Ltd.

Chapter 2 Troubleshooting Flowchart

The flow of troubleshooting when an error occurs in Hitachi Data Ingestor is described.
The troubleshooting flowchart indicates the determination of the failure content after detecting a failure by the procedures described in chapter 1, checking method for the failure, and the direction of the maintenance procedure.

The determination process is different by the configuration of a cluster or a single node.
For the cluster configuration, refer to "C.2.2.1 Failure determination procedure at the Cluster Configuration", and for the single node configuration, refer to "C.2.2.2 Failure determination procedure at the single node configuration".

If the model to be maintained is unknown, refer to "A.2.1 Front side" and determine based on the shape of the front side of the node.

Copyright © 2011, 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

Chapter 3 Maintenance Procedure of Power Supply Failures

The maintenance procedure of power supply failures is described.

The determination process is different by the configuration of a cluster or a single node.
For the cluster configuration, refer to "C.2.3.1.1 Procedure for determining power supply failures in the cluster configuration", and for the single node configuration, refer to "C.2.3.1.2 Procedure for determining power supply failures in the single node configuration".

3.1 Maintenance Procedure at the Time of the Dual Failure of the Power Supply

The maintenance procedure at the time of the dual failure of the power supply occurred in the cluster configuration is described in the following.

At the time of dual failure of the power supply, the node where a failure occurred may be in the suspended state and be forcibly performed failover to the other side node. Therefore, after removing the cables for heartbeat port and the maintenance port on the node where the failure occurred, execute the following procedures.
When both power source lamps indicate error (*) or are turned off, the node is not receiving power. In that case, request the system administrator to check the commercial power supply and if there is no problem on the power supply, replace the two of power supply units or two of AC Cables. To replace the two power units, the replacement is performed with the offline mode.

*: For the display status of power source lamp, refer to "A.2.2.1 Power source unit."
For offline replacement of the power supply units, refer to the step (b) and (c) in "D.1.1.1 Replacing the Power Supply Unit (cluster configuration) (2) Replacement procedure while the node is turned off".

After the replacement, perform the following recovery procedure.

(1) After completing the power unit replacement, turn on the power button.

(2) Confirm that the OS startup of the node is completed. Connect the node where power supply units or AC Cables were replaced to KVM or the maintenance PC, and confirm that the logon prompt is displayed on the console window. For the confirmation method, refer to "Set up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)".

(3) Check if there are any other failures. Connect the maintenance PC to the maintenance port, and then execute the hwstatus command to confirm that there are no other failures other than "mng0", "hb0", "pm1", and "collection" of "BMC Information", and execute fpstatus command to confirm that there are no other failures other than the failure on the path status. If there is a failure, contact the support center and execute recovery of the failure part. And then, execute from the step (4).
For the details of hwstatus command, refer to "B.3.1 Displaying the Hardware Status (hwstatus)", and for the details of fpstatus command, refer to "Maintenance Tool '2.5 Displaying the FC Status (fpstatus) (MNTT 02-0280)".

(4) For the node in which the power source failure occurred, execute the "dumpset --off" command for not to execute the dump collection. For the details about dumpset command, refer to "Maintenance Tool '2.20 Setting whether to Collect Dumps (dumpset)' (MNTT 02-1360)".

(5) Execute the "nasshutdown --force" command, and stop the node in which the power source failure occurred. For the details, refer to "Maintenance Tool '2.28 Terminating the OS of This Side Node (nasshutdown)' (MNTT 02-1740)".

(6) Connect the removed heartbeat cable and the maintenance port cable, and turn the power on. For the details about turning on the power, refer to "Installation '2.1.1 Procedure for turning on the power' (INST 02-0000)".

Copyright © 2010, 2014, Hitachi, Ltd.

(7) After completing the startup, the node is automatically reset from the other side node. 10 minutes later from the power-on operation at the step (6), check that "KAQK39507-E" is output after "KAQK39500-E OS error detail=00 00 03 00, Level=00, Type=0D" and "KAQG72028-W" were output on the other side node. For the details of the confirmation of SIM message, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)". If the above SIMs are not output, contact to the support center.

(8) Confirm that the OS startup of the node is complete.
Refer to "Set Up '1.3 Startup Confirmation of the OS by using KVM' (SETUP 01-0010)" and confirm that the login prompt window is displayed.

(9) If a motherboard was replaced when a cable is not connected to heartbeat port and management port of the node which OS has been down, take the following procedures from (a) to (c).

(a) Set the account of BMC. For the setting of an account, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(b) Check the information of the BMC interface. Check if the information is not changed with the written information before replacing the motherboard.
If the information has been changed, set to the information as the written information before replacing the mother board again.
For the setting of the BMC interface information, refer to "Maintenance Tool '2.18 Setting BMC LAN Information (bmcctl)' (MNTT 02-1210)".

(c) Execute the timeget command in the both node with no option specifying, and check that the present time matches in the both nodes. For the confirmation of the present time, make sure that the "Year, month, date, hour, and minute" are matched. For the present time confirmation, refer to "Maintenance Tool '2.42 Acquisition of Time/Time Zone (timeget)' (MNTT 02-2430)".
If they are not matched, set the time with following procedure. Rebooting is required after the time setting.
To replace the node, refer to "Set Up '9.1 UTC-based Time Setting' (SETUP 09-0000)" and acquire the current time from the node which has not been replaced using the timeset command, and set the value to the maintenance PC.
See the current time of the maintenance PC on the replace node to reset the current time of the node using the timeset command. For the details of the current time setting, refer to "Maintenance Tool '2.43 Time Setting (timeset)' (MNTT 02-2470)".
For the reboot, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".

(10) Execute "dumpset --on" command for the node in which the power source failure occurred, and execute the dump collection. For the dumpset command, refer to "Maintenance Tool '2.20 Setting whether to Collect Dumps (dumpset)' (MNTT 02-1360)".

Copyright © 2012, 2015, Hitachi, Ltd.

(11) After restarting the node that was reset, check the “Node Status” of the node and if it shows “INACTIVE”, request the system administrator to set the “Node Status” of that node to “UP”. After confirming “UP” in the “Node Status”, request the system administrator to perform failback the resource group of the node which has been performed failover.
For the details about the confirmation of “Node Status”, refer to “Maintenance Tool ‘2.2 Displaying the Cluster Status (clstatus)’ (MNTT 02-0040)”.
For the reference place in User’s Guide describing the details about starting a node, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 4 ‘Stopping and starting a node’’ (GENE 00-0040)”, and for the reference place in User’s Guide describing the details about failover/failback of a resource group, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 4 ‘Changing the execution node of a resource group’’ (GENE 00-0040)”.
For the details about starting node, refer to “User’s Guide ‘Stopping and starting a node’”, for the details about failover/failback of the resource group, refer to “User’s Guide ‘Changing the execution node of a resource group’”.
Note that if the system administrator is absent, maintenance personnel should make contact with the system administrator and execute this operation with his/her permission.
For the operation procedure, refer to “Maintenance Tool ‘3.2 Failback and Start of Node after Starting the OS’ (MNTT 03-0030)”.

Copyright © 2013, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2013, Hitachi, Ltd.

Chapter 4 Determination of Management Network Failure

For the determination process of management network failures, refer to "C.2.3.2 Determination of management network failure".

Copyright © 2010, 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, 2011, Hitachi, Ltd.

Chapter 5 Method of Determining Failure Information

This chapter describes the failure notice method and failed part specification of HDI.
If the failure location can be specified by the contents of the failure notice, the maintenance personnel recover the relevant location. If the failure location cannot be specified, specify the failed part by the determination operation.

5.1 Determining FC Path Failures

By the reported SIM message, execute the fpstatus command of the CLI command on both nodes (in the single node configuration, on the local node) to determine the factor of the FC path failure and check the Status (path status) of the output result. In the OS version 3.0.0-XX or later, execute fpstatus command with attaching "-v" option by considering the connection of multiple arrays. In the cluster configuration, attaching "--allnode" option can confirm the both nodes output results with the execution of just one side node. For the confirmation of OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".
Furthermore, the parts to be the replacement target at the time of FC path failures are shown in the following.
Check the device configuration of the customer side and request the order beforehand.

List of parts to be the replacement target:
FC card, FC-SW, FC-SW host connector, array side host connector, FC cable

5.1.1 Path status confirmation method

Execute the fpstatus command of the CLI command on both nodes (in the single node configuration, on the local node), and check the status of the FC path connected to the node.
The port name of the node side differs by the model. Therefore, refer to "A.2.2.2 Port arrangement and port names" and read it as a model to be the target.
The method to specify the FC path failure from the command execution result is described below.

(1) How to write down failure information
Write down the information to specify the FC path failure from the result of fpstatus command execution.
Figure 5.1.1-1 to Figure 5.1.1-4 show examples of FC path failure occurrence in the configuration using FC-SW and without using FC-SW.

Copyright © 2010, 2012, Hitachi, Ltd.

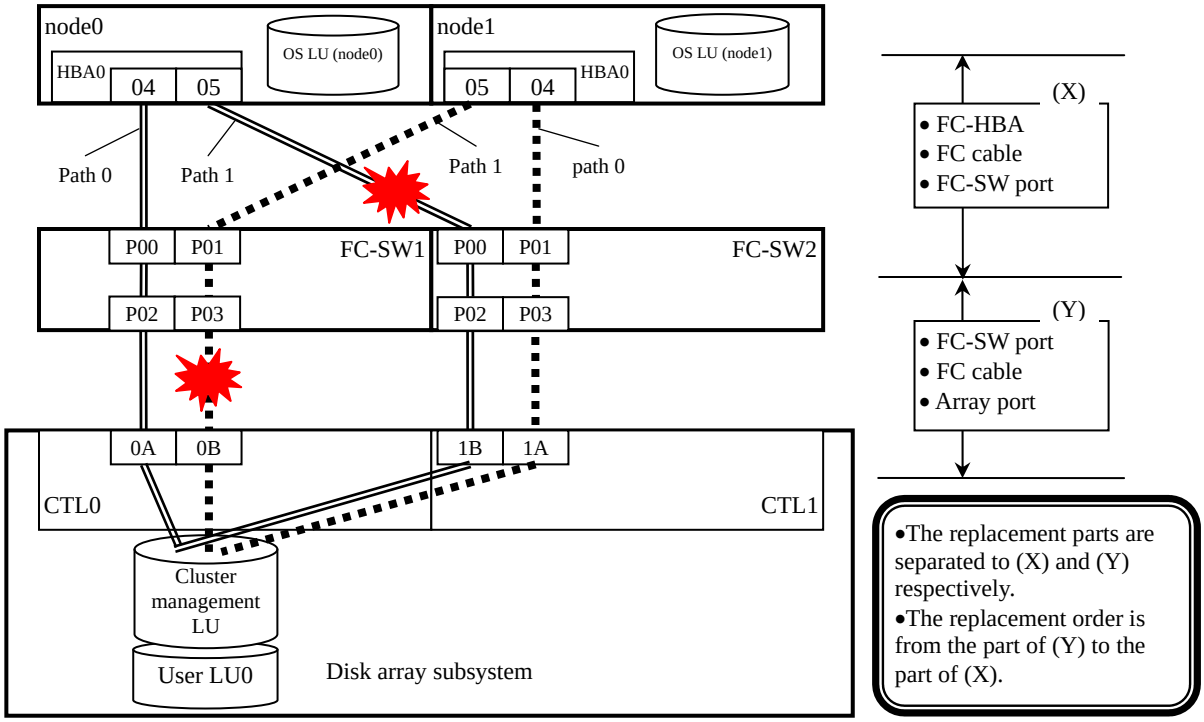


Figure 5.1.1-1 Example of FC Path Failure Occurrence in the configuration using FC-SW

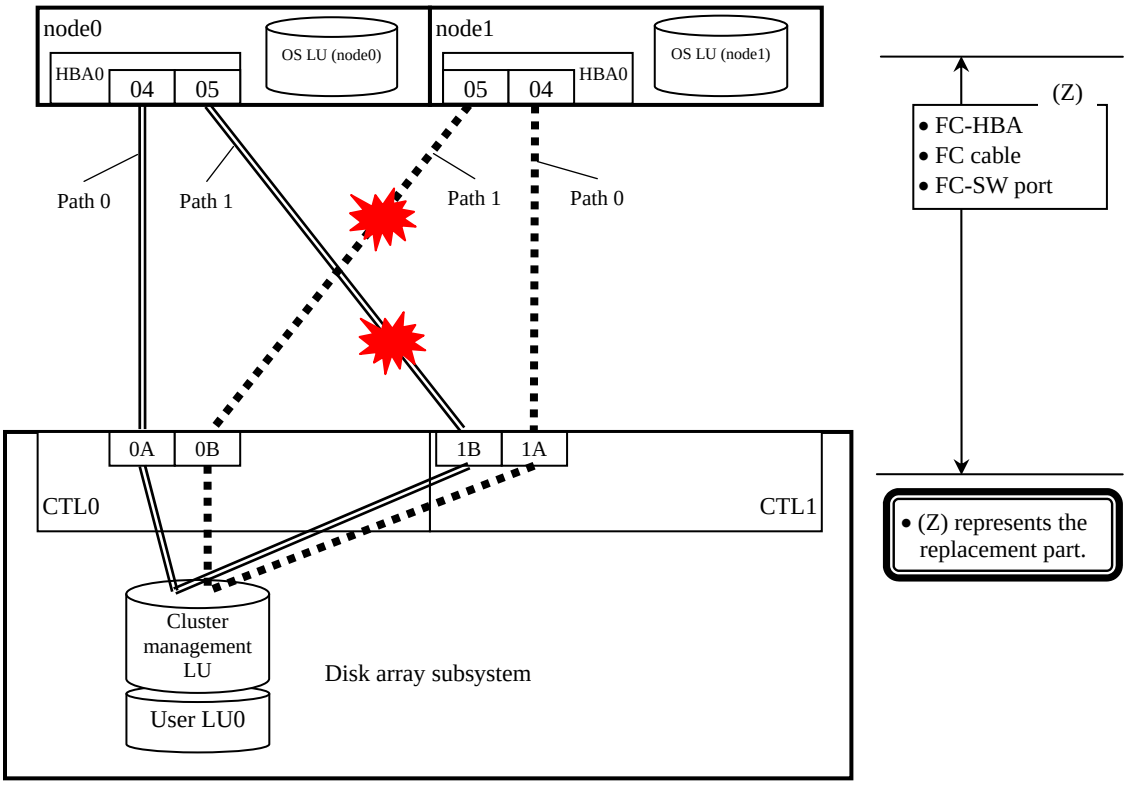


Figure 5.1.1-2 Example of FC Path Failure Occurrence in the configuration without using FC-SW

Copyright © 2010, 2011, Hitachi, Ltd.

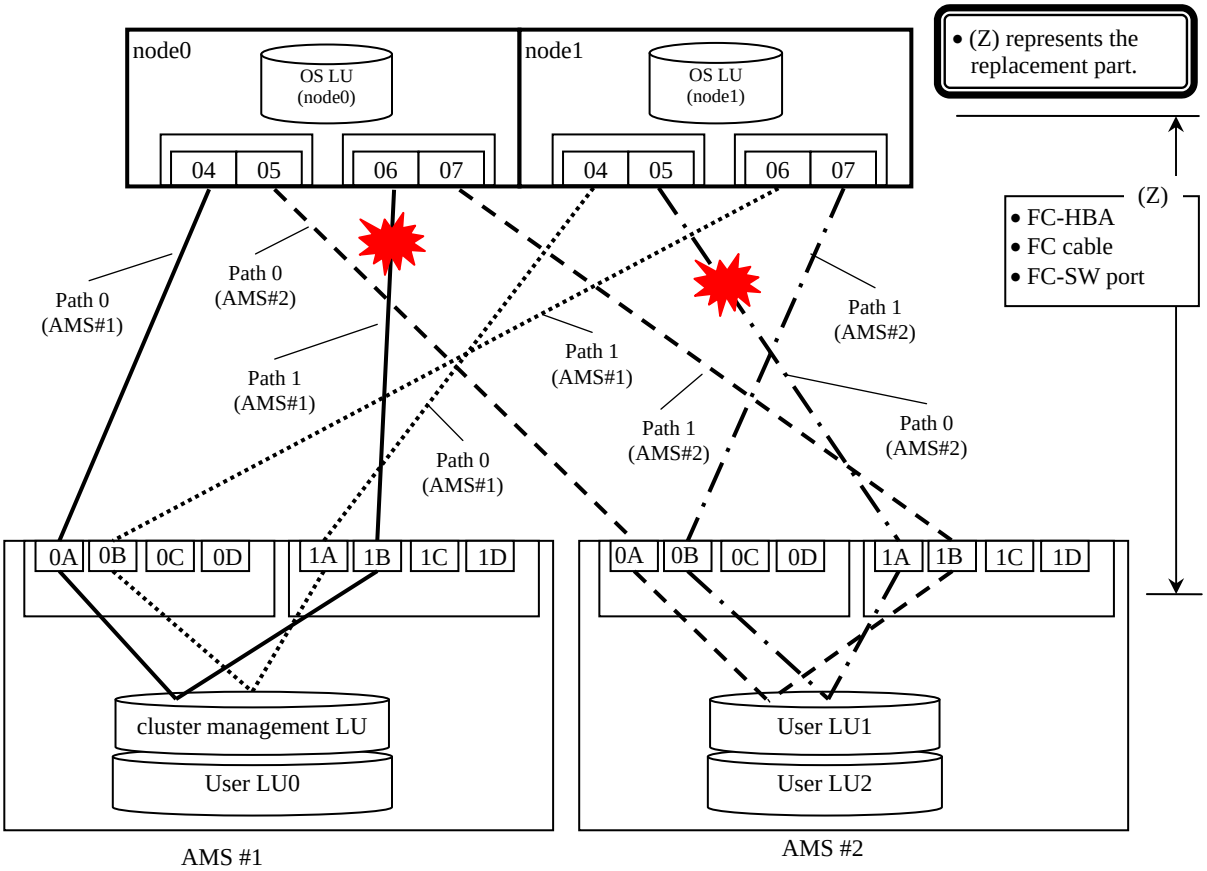


Figure 5.1.1-3 Example of FC Path Failure Occurrence in the configuration using two FC HBAs and two arrays (multi array configuration)

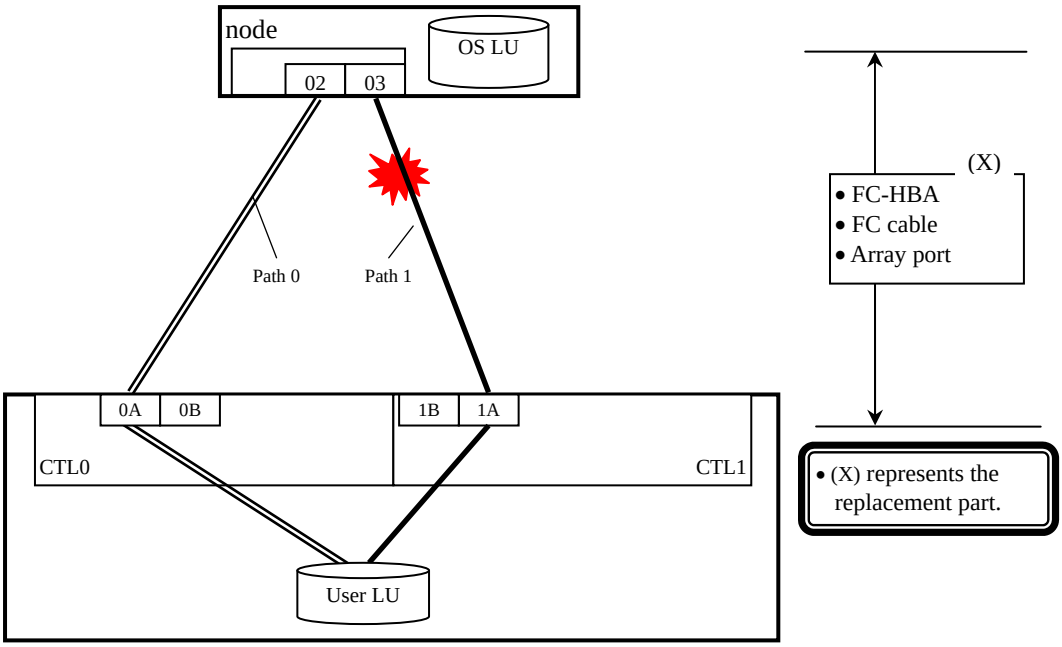


Figure 5.1.1-4 Example of FC Path Failure Occurrence in the Single Node Configuration

Copyright © 2011, 2012, Hitachi, Ltd.

To specify the failure location, write down the path information according to the following procedure.

① Focus on the path whose Status part in the result of executing the fpstatus command is not “Online” status.

② When the path whose Status is not “Online” exists only in one node, the node is called “node to be the target”. When the paths whose Status is not “Online” exist in both nodes, node0 is called “node to be the target”.

③ Write down the path information and the node name. The path information is shown below.
Write down the “Serial” to specify the connection arrays in the multi array configuration.

Path	Target	HostPort	HostPortWWN	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

④ Based on the written path information, perform the failure determination as described in Troubleshooting “5.1.2 Determination by the FC path status in the configuration using FC-SW” (TRBL05-0030) when FC-SW is included in the system configuration of the target connection array. When FC-SW is not included in the system configuration and in the single node configuration, perform the failure determination as described in Troubleshooting “5.1.3 Determination by the FC path status in the configuration without using FC-SW” (TRBL05-0300).

Copyright © 2012, Hitachi, Ltd.

(2) Example of fpstatus command execution

Refer to (2-1) when the OS version is 2.2.1-XX or earlier, and refer to (2-2) when the OS version is 3.0.0-XX or later. There is a case on (2-2) that the communication cannot be done with the target node and the target information may not be displayed on the window. In that case, execute “fpstatus –v” in each node, and then refer to the both nodes information.
For the confirmation of OS version, refer to “Maintenance Tool ‘2.34 Displaying the Version of the OS (versionlist)’ (MNTT 02-2060)”.

(2-1) When the OS version is 2.2.1-XX or earlier

● Example of executing the fpstatus command (at the time of option omitted) in the node to be the target (node0)

```
$ sudo fpstatus
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Status
path000-0004-0A N0-T000  fc0004   10000000c98f26be 0A        50060e800044b632 Online
path000-0005-1B N0-T000  fc0005   10000000c98f36be 1B        50060e8005271c64 Error
```

● Example of executing the fpstatus command (at the time of option omitted) in the node on the opposite side (node1)

```
$ sudo fpstatus
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Status
path000-0004-1A N1-T000  fc0004   10000000c98f27ab 1A        50060e800044b636 Online
path000-0005-0B N1-T000  fc0005   10000000c98f37bc 0B        50060e8005271c68 Error
```

(2-2) When the OS version is 3.0.0-XX or later

● When fpstatus command (with “--allnode” option) is executed on the target node (node0)

```
$ sudo fpstatus --allnode
node0(DJ8RMPBX)
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A N0-T000  fc0004   10000000c98f26be 0A        50060e800044b632 AMS   87010001 Online
path000-0005-1B N0-T000  fc0005   10000000c98f36be 1B        50060e8005271c64 AMS   87010001 Error

node1(D79RMPDX)
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-1A N1-T000  fc0004   10000000c98f27ab 1A        50060e800044b636 AMS   87010001 Online
path000-0005-0B N1-T000  fc0005   10000000c98f37bc 0B        50060e8005271c68 AMS   87010001 Error
```

[Description of FC path information to be written down (description of surrounded part)]

- The ArrayPort names “0A” and “0B” indicate the path connected to the controller 0 side of the array device and this path is described as path 0. “1A” and “1B” indicate the path connected to the controller 1 side of the array device and this path is described as path 1.

- The “Status” becomes “Error” when a failure has occurred in any path connected from the node to the array device.

For the details of the fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

Copyright © 2010, 2012, Hitachi, Ltd.

5.1.2 Determination by the FC path status in the configuration using FC-SW

Based on the written path information, determine the failure in "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)" (TRBL 05-0035) as shown below.

In the OS version is 3.0.0-XX or later, if all the ports are used in the configuration with two FC-cards, the four paths in each node are displayed as shown in the following examples by the combination of the FC-SW zoning. In this case, consider the replacing path that refers to the same LU in each node as one combination, and determine the failure from the path statuses shown in "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)" (TRBL 05-0035). If four paths are displayed in each node, determination process must be done for each replacing path.
The paths to be replaced are the two paths that match the "Target" and "Serial" as shown in the following execution example in each node. (In the execution example in the following, it is "N0-T000" and "N0-T001" in node0, and "N1-T000" and "N1-T001" in node1.)

There is another replacing path that refers to the same LU in the other side node. In the following examples, ① and ② are the combination of the replacing path that refers to the same LU.

However, when the path status is "Unknown" or "Configuration Mismatch", all the path status might not be displayed, or "Target" or "Serial" might not be displayed. Therefore, when the path status is "Unknown" or "Configuration Mismatch", follow the instruction described in Troubleshooting "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (2/2)" (TRBL 05-0040).

- Execution example when all the ports are used in the configuration using two FC cards.

[A case that connecting four paths in the same array]

Execution example at node0

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial   Status
① path000-0004-0A   N0-T000  fc0004   10000000c98f26be 0A        50060e800044b632 AMS   87010001 Online
  path000-0006-1A   N0-T000  fc0006   10000000c98f36be 1A        50060e800044b636 AMS   87010001 Error
  path001-0004-0B   N0-T001  fc0004   10000000c98f26be 0B        50060e8005271c72 AMS   87010001 Online
  path001-0006-1B   N0-T001  fc0006   10000000c98f36be 1B        50060e8005271c76 AMS   87010001 Online
```

Execution example at node1

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial   Status
② path000-0004-1A   N1-T000  fc0004   10000000c98f27ab 1A        50060e800044b636 AMS   87010001 Online
  path000-0006-0A   N1-T000  fc0006   10000000c98f37bc 0A        50060e800044b632 AMS   87010001 Online
  path001-0004-1B   N1-T001  fc0004   10000000c98f27ab 1B        50060e8005271c76 AMS   87010001 Error
  path001-0006-0B   N1-T001  fc0006   10000000c98f37bc 0B        50060e8005271c72 AMS   87010001 Online
```

Copyright © 2010, 2012, Hitachi, Ltd.

[A case of multiple arrays configuration]

Execution example at node0

```
$ sudo fpstatus - v
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A     N0-T000   fc0004   10000000c98f26be  0A        50060e8005271c62  AMS   87010001   Online
path000-0006-1A     N0-T000   fc0006   10000000c98f36be  1A        50060e8005271c60  AMS   87010001   Error
path001-0004-0A     N0-T001   fc0004   10000000c98f26be  0A        50060e8005238b68  AMS   87010010   Online
path001-0006-1A     N0-T001   fc0006   10000000c98f36be  1A        50060e8005238b64  AMS   87010010   Online
```

Execution example at node1

```
$ sudo fpstatus - v
Path                Target    HostPort HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-1A     N1-T000   fc0004   10000000c98f27ab  1A        50060e8005271c60  AMS   87010001   Online
path000-0006-0A     N1-T000   fc0006   10000000c98f37bc  0A        50060e8005271c62  AMS   87010001   Online
path001-0004-1A     N1-T001   fc0004   10000000c98f27ab  1A        50060e8005271b64  AMS   87010010   Error
path001-0006-0A     N1-T001   fc0006   10000000c98f37bc  0A        50060e8005271b68  AMS   87010010   Online
```

When the OS version is 3.0.0-XX or later, specifying “--allnode” to fpstatus command can refer to the path information of the both nodes. However, when the communication cannot be done with the other side node, the information of the other side node may not be displayed. In this case, specify “-v” option to fpstatus in each node, and refer to the both nodes information. For the confirmation of the OS version, refer to “Maintenance Tool ‘2.34 Displaying the Version of the OS (versionlist)’ (MNTT 02-2060)”.
For the details about fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

The next page shows the identifying method of the combination of paths when the four or more FC path information excepting “Unknown” and “Configuration Mismatch” are displayed as shown in the above path information.

Copyright © 2011, 2012, Hitachi, Ltd.

In the determination table shown in Troubleshooting "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)" (TRBL 05-0035), determination is done by using a combination of the path information that refers to the same LU between the target node and the other side node. Therefore, it is required to identify the path information that refers to the same LU in each node or that refers to the same LU between the nodes.
The method of identifying the path information that refers to the same LU is described below when the fpstatus execution example of each node are the following.

Execution example at node0

$ sudo fpstatus - v

	Path	Target	HostPort	HostPortWWN	ArrayPort	ArrayPortWWN	Model	Serial	Status
①	path000-0004-**0A**	N0-T000	fc0004	10000000c98f26be	**0A**	50060e800044b632	AMS	87010001	**Online**
	path000-0006-**1A**	N0-T000	fc0006	10000000c98f36be	**1A**	50060e800044b636	AMS	87010001	**Error**
	path001-0004-**0B**	N0-T001	fc0004	10000000c98f26be	**0B**	50060e8005271c72	AMS	87010001	**Online**
	path001-0006-**1B**	N0-T001	fc0006	10000000c98f36be	**1B**	50060e8005271c76	AMS	87010001	**Online**

Execution example at node1

$ sudo fpstatus - v

	Path	Target	HostPort	HostPortWWN	ArrayPort	ArrayPortWWN	Model	Serial	Status
②	path000-0004-**1A**	N1-T000	fc0004	10000000c98f27ab	**1A**	50060e800044b636	AMS	87010001	**Online**
	path000-0006-**0A**	N1-T000	fc0006	10000000c98f37bc	**0A**	50060e800044b632	AMS	87010001	**Online**
	path001-0004-**1B**	N1-T001	fc0004	10000000c98f27ab	**1B**	50060e8005271c76	AMS	87010001	**Error**
	path001-0006-**0B**	N1-T001	fc0006	10000000c98f37bc	**0B**	50060e8005271c72	AMS	87010001	**Online**

1. Verify the replacing path in each node. The replacing paths have the path information where "Target" is the same.
   On the above example, the first path is the path that contains "N0-T000" and the second path is the path that contains "N0-T001" in the node0. In the same manner, the first path is the path that contains "N1-T000" and the second path is the path that contains "N1-T001" in the node1.
2. Next, identify the path combination that refers to the same LU between the node0 and node1. [In the case of multi-array configuration] shown in "TRBL 05-0031" four paths in each node are displayed but the "Serial" is different in each replacing part. Therefore, ① and ② that match the "Serial" in the both nodes can be identified that it refers to the same LU between the nodes. After the identification, proceed to step3.
   However, if "Serial" of the replacing path is the same as shown in the above example, it is needed to identify the path information that refers to the same LU with either method of the following.
   The first method is to execute fpstatus command with "--lupath" option. ((1) A method of using fpstatus command to identify the same LU between the nodes.)
   For fpstatus command, refer to "Maintenance Tool '2.5 Displaying the FC Status (fpstatus)' (MNTT 02-0280)".
   The second method is to identify with "Maintenance Tool '2.35 Displaying the LU Information in the Disk Array Subsystem (alulist)' (MNTT 02-2090)". ((2) A method of using alulist command to identify the path that refers to the same LU between the nodes.)
   The determination method is described from the next page.
3. Write down the FC path information of the both nodes that refer to the same LU identified at the step "2".

Copyright © 2011, Hitachi, Ltd.

4. Based on the path that identified in the above description, execute the determination operation by confirming the FC path status of ① as the target node and of ② as the other side of the node from Troubleshooting "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)" (TRBL 05-0035). In the execution example in "TRBL 05-0032" execute the determination operation of #1 as the path0 and path1 of the target node is "Online" and "Error" respectively, and the path0 and path1 on the other side node is "Online" and "Online" respectively.
5. After completing the step "4," check the status of the other side replacing path, and if there is a path that the status is not in "Online," execute the step "2" and "3". In the execution example in "TRBL 05-0032" execute the determination procedure of #2 as the path0 and path1 of the target node is "Online" and "Error" respectively, and the path0 and path1 of the other side node is "Error" and "Online" respectively.

Copyright © 2011, Hitachi, Ltd.

(1) A method of using fpstatus command to identify the same LU between the nodes
Since this procedure cannot be done in the OS version before 3.0.0-XX, execute Troubleshooting "5.1.2 (2) A method of using alulist command to identify the path that refers to the same LU between the nodes" (TRBL 05-0034).
For the confirmation of the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)'(MNTT 02-2060)".

(a) Execute "fpstatus –lupath" in either of the nodes. Figure 5.1.2-A is an execution example at the side of node0. The LU information of both nodes can be displayed. However, if the communication cannot be done with the other side node, the information of the other side node may not be displayed. In this case, execute the procedure described in Troubleshooting "5.1.2 (2) A method of using alulist command to identify the path that refers to the same LU between the nodes" (TRBL 05-0034).

```
$ sudo fpstatus –lupath
Model   Serial LDEV(  hex)  ArrayPort Target   HostPort  HostPortWWN      Status      Mismatch
AMS     87010001 11( 000B) 0A      N0-T000  fc0004    10000000c98f26be Online      -
AMS     87010001 11( 000B) 1A      N0-T000  fc0006    10000000c98f36be Offline(E)   (1)
AMS     87010001 11( 000B) 1A      N1-T000  fc0004    10000000c98f27ab Online      -
AMS     87010001 11( 000B) 0A      N1-T000  fc0006    10000000c98f37bc Online      -
AMS     87010001 21( 0015) 0A      N0-T000  fc0004    10000000c98f26be Online      -
AMS     87010001 21( 0015) 1A      N0-T000  fc0006    10000000c98f36be Offline(E)     -
AMS     87010001 21( 0015) 1A      N1-T000  fc0004    10000000c98f27ab Online      -
AMS     87010001 21( 0015) 0A      N1-T000  fc0006    10000000c98f37bc Online      -
AMS     87010001 31( 001F) 0B      N0-T001  fc0004    10000000c98f26be Online      -
AMS     87010001 31( 001F) 1B      N0-T001  fc0006    10000000c98f36be Online      -  (2)
AMS     87010001 31( 001F) 1B      N1-T001  fc0004    10000000c98f27ab Offline(E)     -
AMS     87010001 31( 001F) 0B      N1-T001  fc0006    10000000c98f37bc Online      -
AMS     87010001 41( 0029) 0B      N0-T001  fc0004    10000000c98f26be Online      -
AMS     87010001 41( 0029) 1B      N0-T001  fc0006    10000000c98f36be Online      -
AMS     87010001 41( 0029) 1B      N1-T001  fc0004    10000000c98f27ab Offline(E)     -
AMS     87010001 41( 0029) 0B      N1-T001  fc0006    10000000c98f37bc Online      -
```

Figure 5.1.2-A fpstatus Execution Example

(b) The LU path information of the both nodes is sorted in the order of "Serial" and "LDEV" as shown above. As in the thick frames on the above figure, four path information that refer to the same "LDEV" are displayed.
Looking at (1) in the above figure, "N0-T000" and "N1-T000" shown in "Target" can be confirmed as the path that refer to the same LU.
In the same manner, when looking at (2) in the above figure, "N0-T001" and "N1-T001" shown in "Target" can be confirmed as the path that refer to the same LU.

(c) From the result of (b), the path information that refers to the same LU is the path information of ①that includes "N0-T000" and the path information of ② that includes "N1-T000" in the execution example as shown in "TRBL 05-0032".
In the same manner, the other path information (a pair of "N0-T001" and "N1-T001") can be identified.
After the identification, proceed to step 3.

Copyright © 2011, 2012, Hitachi, Ltd.

(2) A method of using alulist command to identify the path that refers to the same LU between the nodes

(a) Compare the result of alulist command in the both nodes. Figure 5.1.2-B shows an execution example on the side of node0, and Figure 5.1.2-C shows an execution example on the side of node1. In each node, the LU information of one side ArrayPort of the replacing path is displayed.

```
$ sudo alulist
model    serial      LDEV(  hex)  port   type    size
AMS      87010001     0(  0000)   0A     SATA    70.000GB
AMS      87010001     3(  0003)   0A     SATA    30.000GB
• • • •
AMS      87010001    20(  0014)   0B     SATA    20.000GB
AMS      87010001    22(  0016)   0B     SATA    20.000GB
```

Figure 5.1.2-B Execution example of alulist on node0

(1)

(2)

```
$ sudo alulist
model    serial      LDEV(  hex)  port   type    size
AMS      87010001     0(  0000)   1A     SATA    70.000GB
AMS      87010001     3(  0003)   1A     SATA    30.000GB
• • • •
AMS      87010001    20(  0014)   0B     SATA    20.000GB
AMS      87010001    22(  0016)   0B     SATA    20.000GB
```

Figure 5.1.2-C Execution example of alulist on node1

(b) Identify “port” that refers to the same “LDEV” in both nodes. In the above diagram, “0A” on the side of node0 and “1A” on the side of node1from the “port” that refers to “0” of “LDEV” that is enclosed in (1) can be identified the ArrayPort that refers to the same LU in each node. In the same manner, “0B” on the side of node0 and “0B” on the side of node1 from the “port” that refers to “20” of “LDEV” that is enclosed in (2) can be identified the ArrayPort that refers to the same LU in each node.

(c) Identifying the one side of ArrayPort that refers to the same LU between the nodes in the step (b) can identify a combination of replacing path.
The ArrayPort “0A” on the side of node0 that is identified at (b) is included in the thick frame ① of the replacing path of node0 from the execution example as described in “TRBL 05-0032”. And the replacing path of node1 to be paired with that is the thick frame ② of the replacing path that includes ArrayPort “1A” of the node 1 identified at (b).
With the above information, ① and ② in the execution example described in “TRBL 05-0032” can be identified as the path information that refers to the same LU.
In the same manner, the other side path information can be identified.
After the identification, proceed to step 3.

Copyright © 2011, Hitachi, Ltd.

Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)

#	FC path status after fpstatus command execution		Assumed failure	Determination continuing flow
	node to be the target	node on opposite side		
1 (*1)	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Online	A failure has occurred in any of FC card, FC port, FC cable, FC-SW port (at the time of FC-SW configuration) and array port.	To the flow in Figure 5.1.2-1 (TRBL05-0050)
	Path 0 : Online Path 1 : Error	Path 0 : Online Path 1 : Online		
2 (*1)	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Error	• An FC-SW failure has occurred. • A failure on the array controller side has occurred. • A dual failure of No.1 has occurred.	To the flow in Figure 5.1.2-2 (TRBL05-0090)
	Path 0 : Online Path 1 : Error	Path 0 : Error Path 1 : Online		
	Path 0 : Error Path 1 : Online	Path 0 : Error Path 1 : Online		
	Path 0 : Online Path 1 : Error	Path 0 : Online Path 1 : Error		
3	Path 0 : Error Path 1 : Error	Path 0 : Online Path 1 : Online	• An FC card failure of the local node has occurred. • A dual failure of FC-SW port (at the time of FC-SW configuration).	To the flow in Figure 5.1.2-3 (TRBL05-0130)
If a FC path status other than the above #1 to #3 is displayed, determine a failure based on the written downed path information in reference to "Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (2/2)" (TRBL 05-0040).				

*1: When one side status of the FC path is "Configuration Mismatch", and the other side state of the FC path is not displayed as described below, determine it as "Configuration Mismatch" = "Online", and "No display" = "Error". (This status is shown when the OS is restarted after the path failure.)

FC path status after fpstatus command execution			FC path status after fpstatus command execution	
node to be the target	node on opposite side		node to be the target	node on opposite side
Path 0 : No display Path 0 : Configuration Mismatch	Path 0 : Online Path 1 : Online	=	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Online

If this state occurs after replacing HBA, there might be a mistake in inputting the WWN in the setting of the host group security of the disk array subsystem. Check the setting on the side of the disk array subsystem.
If the WWN setting is wrong, correct it, and reboot the node in which the WWN setting was wrong. For the reboot method, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".
If there is no problem on the setting of the disk array subsystem, go to the determination procedure.

Copyright © 2011, Hitachi, Ltd.

Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (2/2)

#	FC path status after fpstatus command execution		Assumed failure	Determination continuing flow
	node to be the target	node on opposite side		
4 (*2)	Path 0 : Error Path 1 : Error	Path 0 : Error Path 1 : Error	• A dual failure of the array power supply has occurred. • Operation error (array shutdown) • A dual failure occurs on FC-SW. • A dual failure occurs on FC card. * A dual failure of the array controller 0/1 has occurred.	To the flow in Figure 5.1.2-5 (TRBL05-0250)
5	Including “Unknown”		An FC card failure of the local node has occurred.	To the flow in Figure 5.1.2-6 (TRBL05-0270)
6	“Configuration Mismatch” is included (However, execute #5 if “Unknown” is included.)		• Operation error (setting error at the time of adding zoning or mapping) • Executed fpstatus command after the OS reboot when the path failure occurred.	(7) Determining failure recovery of case #6 in the table of determination (TRBL05-0280)
7	“Offline” or “Partially Online” exists		Forgetting the procedure after the manual operation and others	(8) Determining failure recovery of case #7 in the table of determination (TRBL05-0290)
8	Combination other than that		The disk array trouble or the dual failure of the device has occurred. Or the FC path failure is recovered.	(9)Determining failure recovery of case #8 in the table of determination (TRBL05-0290)

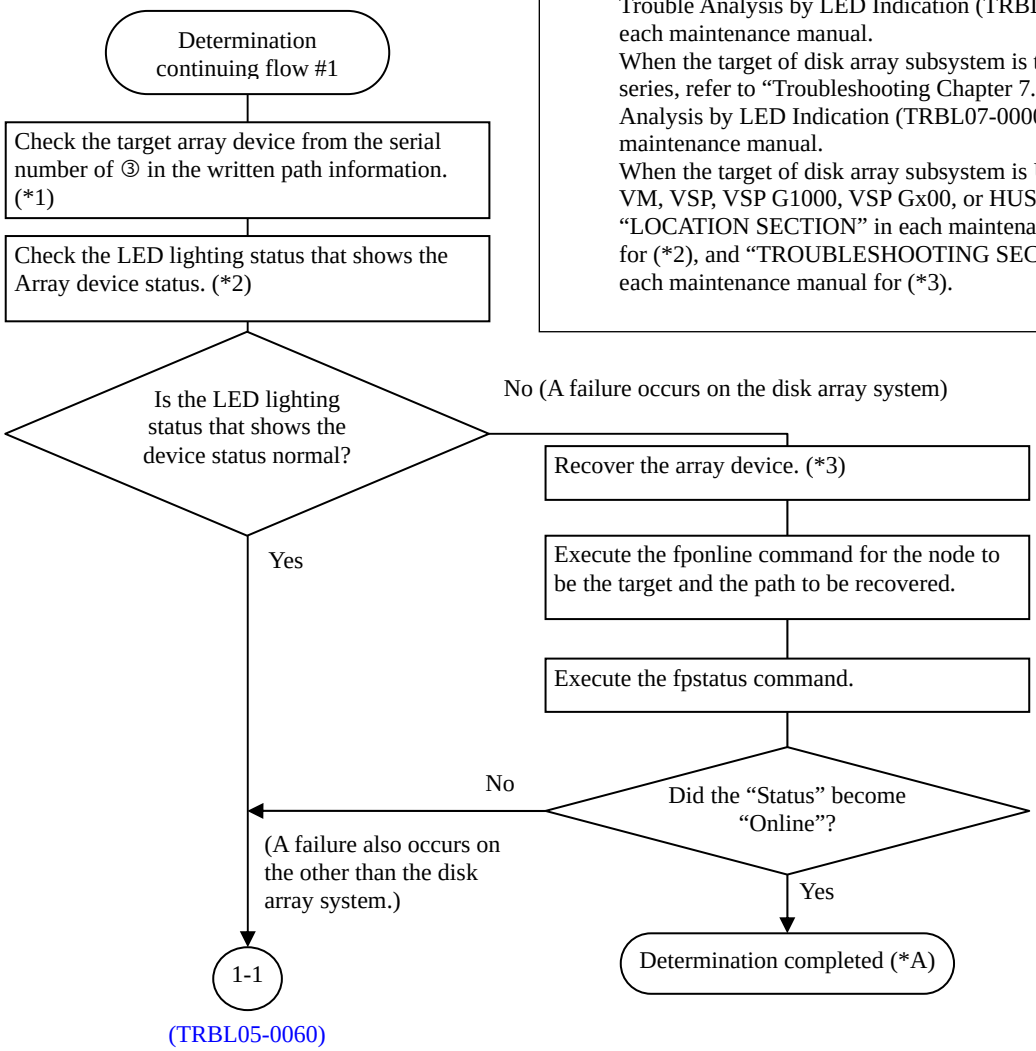
*2: If this state occurs after replacing HBA, there might be a mistake in inputting the WWN in the setting of the host group security of the disk array subsystem. Check the setting on the side of the disk array subsystem.
If the WWN setting is wrong, correct it, and reboot the node in which the WWN setting was wrong. For the reboot method, refer to “Maintenance Tool ‘2.29 Rebooting the OS of This Side Node (nasreboot)’ (MNTT 02-1790)”.
If there is no problem on the setting of the disk array subsystem, go to the determination procedure.

Copyright © 2010, 2014, Hitachi, Ltd.

(1) Determining failure recovery of case #1 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

*1: This is not required when the OS version is 3.0.0-XX or earlier.
*2,*3: When the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual.
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual for (*2), and "TROUBLESHOOTING SECTION" in each maintenance manual for (*3).

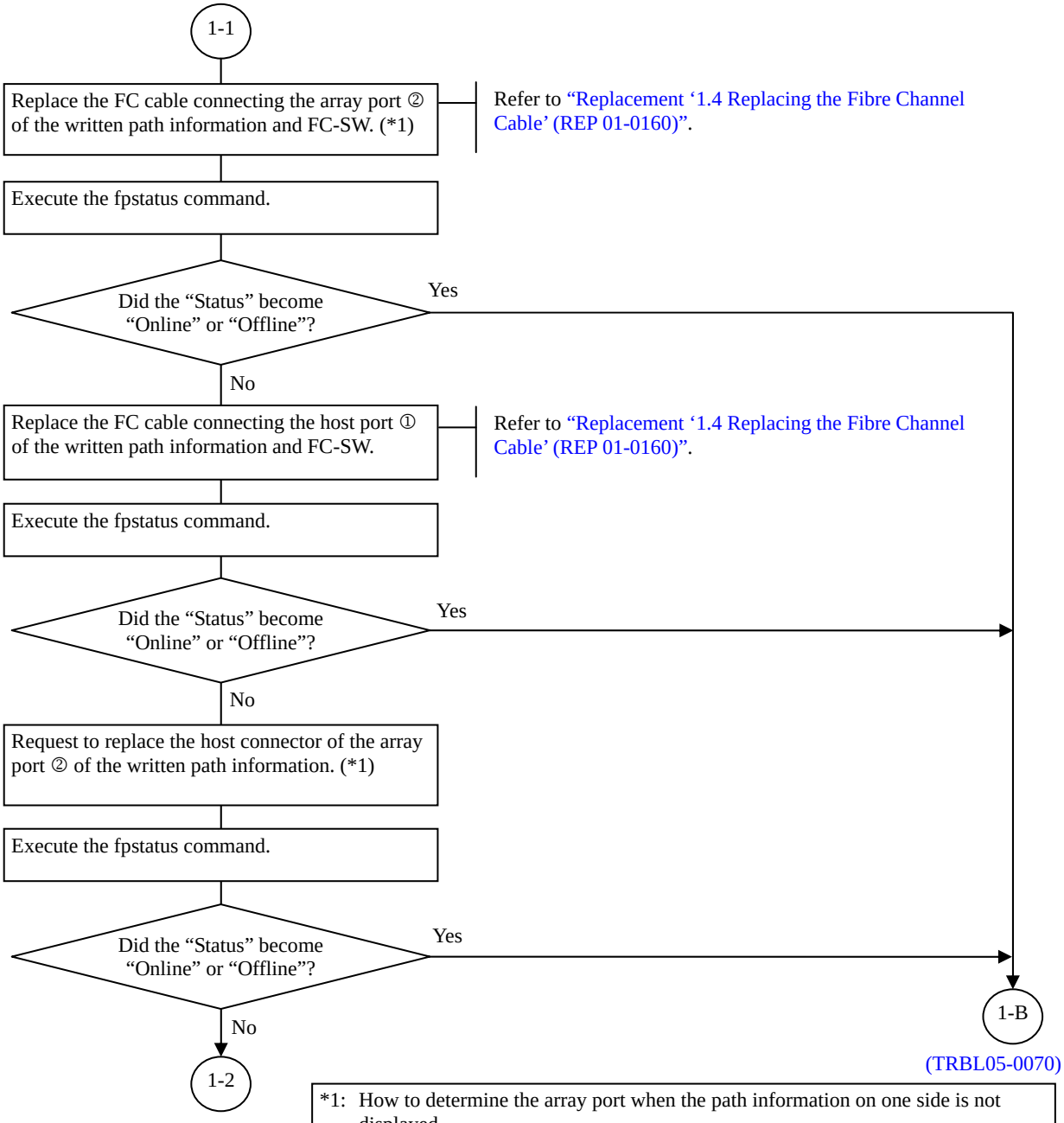


*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online," execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure in the cluster configuration".

Figure 5.1.2-1 Procedure 1 for Determining by FC Path Status (1/4)

Copyright © 2010, 2015, Hitachi, Ltd.

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error



*1: How to determine the array port when the path information on one side is not displayed

(a) Execute the fchbafwlist command, and write down the displayed "Portname". For more details, refer to "Maintenance Tool '2.24 Checking the HBA Firmware Version (fchbafwlist)' (MNTT 02-1600)".

(b) Compare the information of "HostPortWWN" that is displayed by the fpstatus command and the one that is written down at the step (a), and determine the Portname which is not shown on the display.

(c) In the host group security of the disk array subsystem, determine the array port which has the same WWN as the Portname not shown on the display.

Figure 5.1.2-1 Procedure 1 for Determining by FC Path Status (2/4)

Copyright © 2010, 2014, Hitachi, Ltd.

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

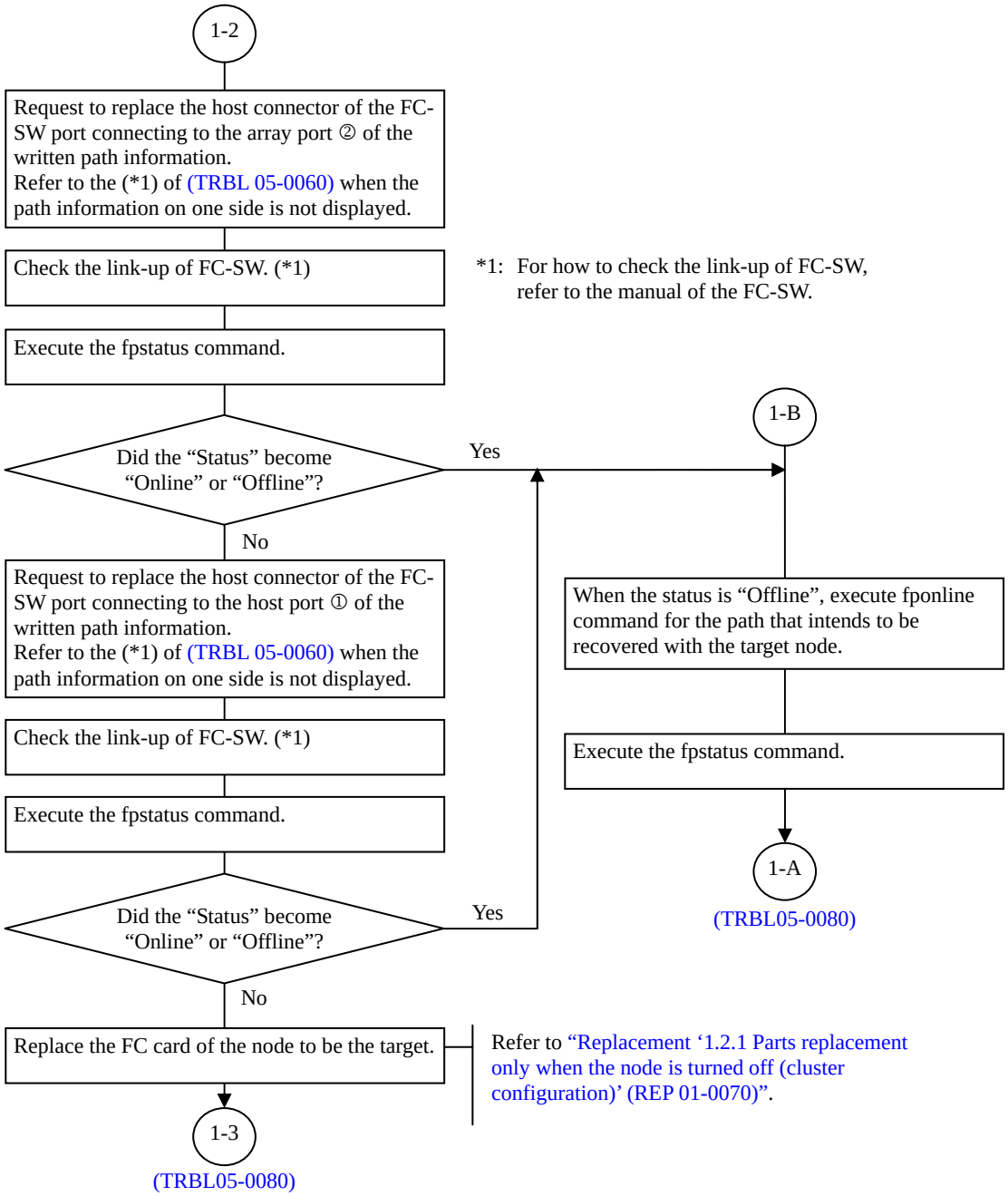
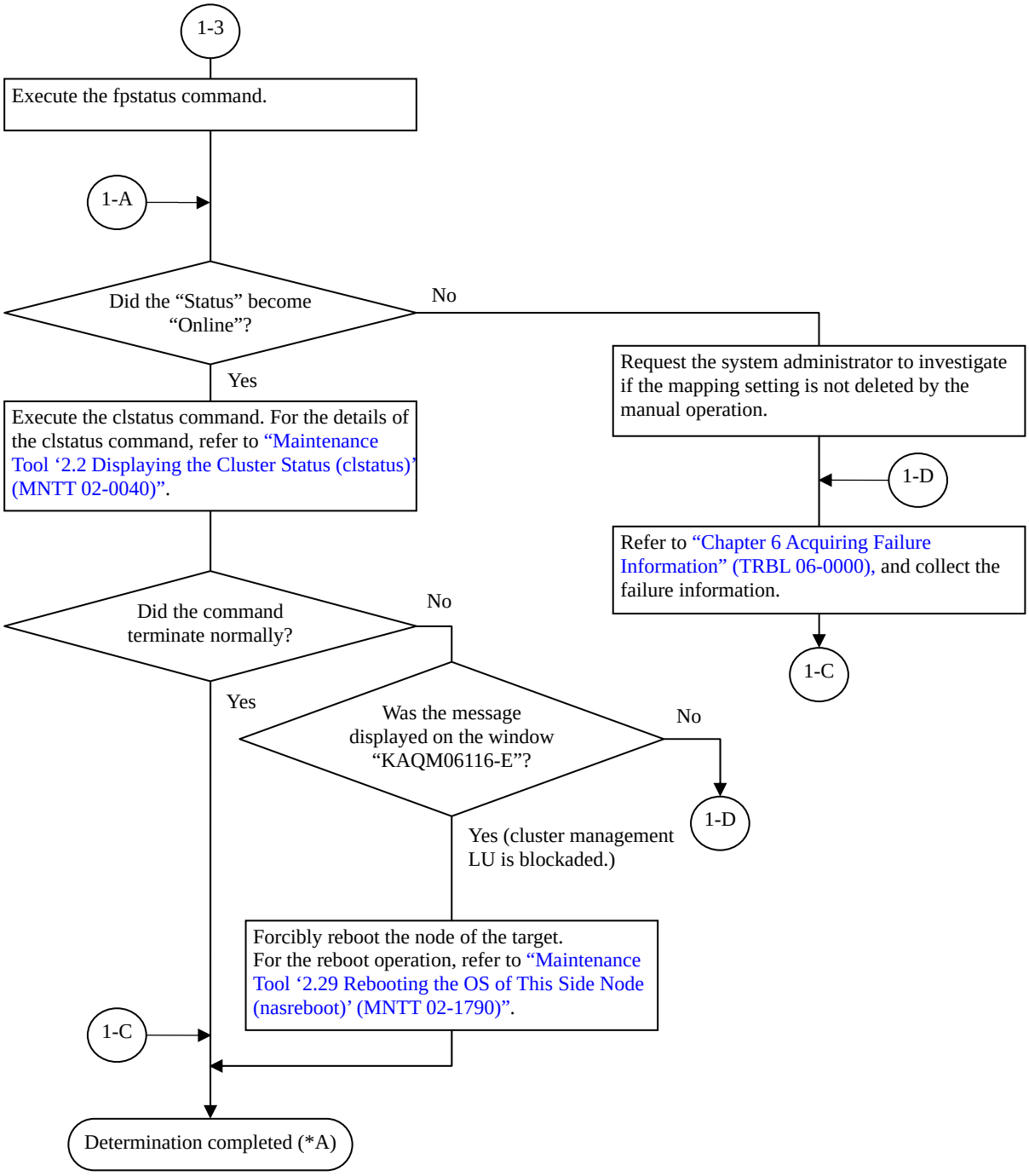


Figure 5.1.2-1 Procedure 1 for Determining by FC Path Status (3/4)

Copyright © 2010, 2011, Hitachi, Ltd.



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online", execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure at the cluster configuration".

Figure 5.1.2-1 Procedure 1 for Determining by FC Path Status (4/4)

Copyright © 2010, 2011, Hitachi, Ltd.

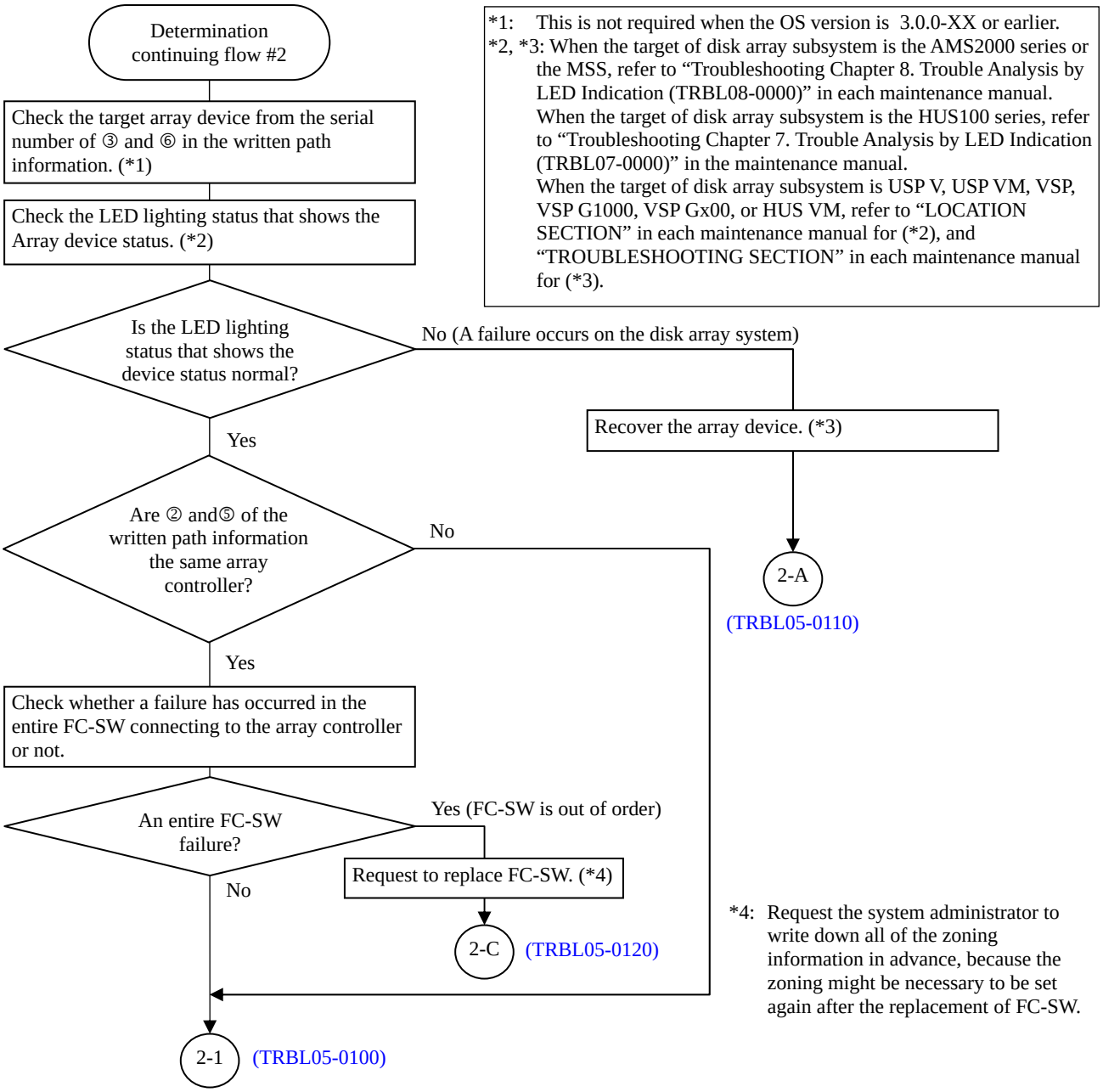
(2) Determining failure recovery of case #2 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	③ Model	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	④ HostPort	HostPortWWN	⑤ ArrayPort	ArrayPortWWN	⑥ Model	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f26ce	1B	50060e8005271c62	AMS	87010001	Error



*1: This is not required when the OS version is 3.0.0-XX or earlier.
*2, *3: When the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual.
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual for (*2), and "TROUBLESHOOTING SECTION" in each maintenance manual for (*3).

*4: Request the system administrator to write down all of the zoning information in advance, because the zoning might be necessary to be set again after the replacement of FC-SW.

Figure 5.1.2-2 Procedure 2 for Determining by FC Path Status (1/4)

Copyright © 2010, 2015, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model ③	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	HostPort ④	HostPortWWN	ArrayPort ⑤	ArrayPortWWN	Model ⑥	Serial	Status
path000-0005-0B	N0-T000	fc0005	10000000c98f26ce	0B	50060e8005271c62	AMS	87010001	Error

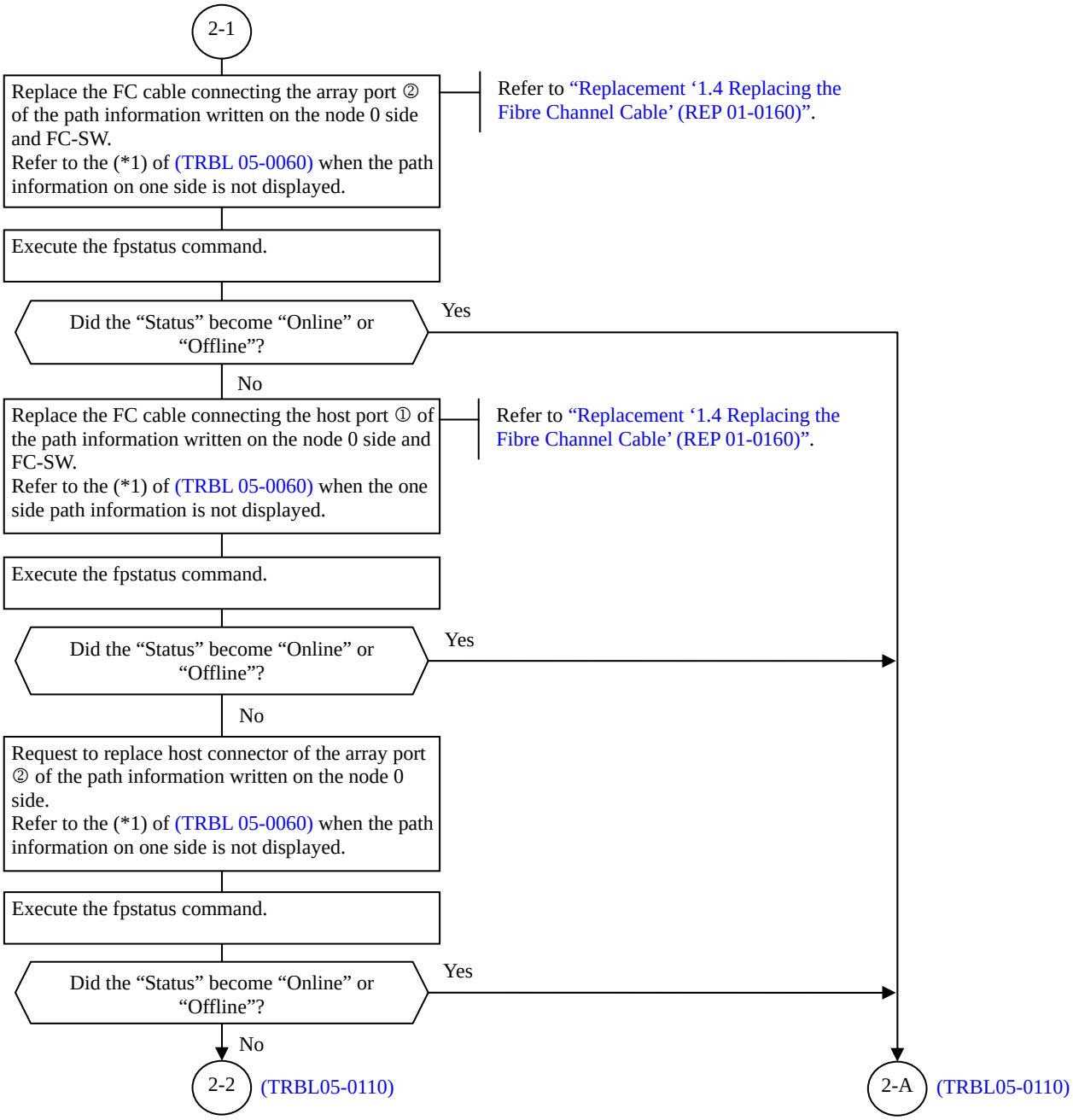


Figure 5.1.2-2 Procedure 2 for Determining by FC Path Status (2/4)

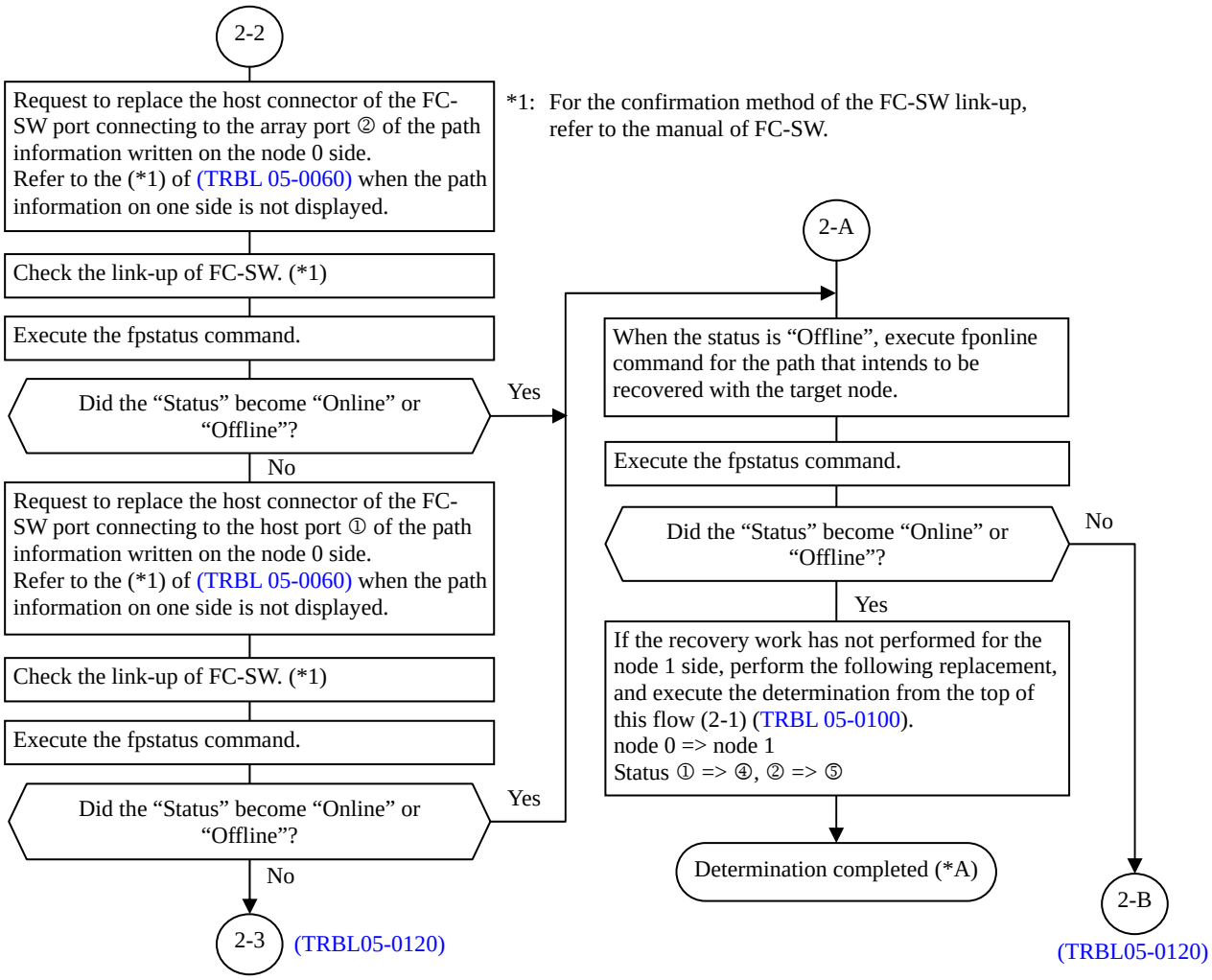
Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model ③	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

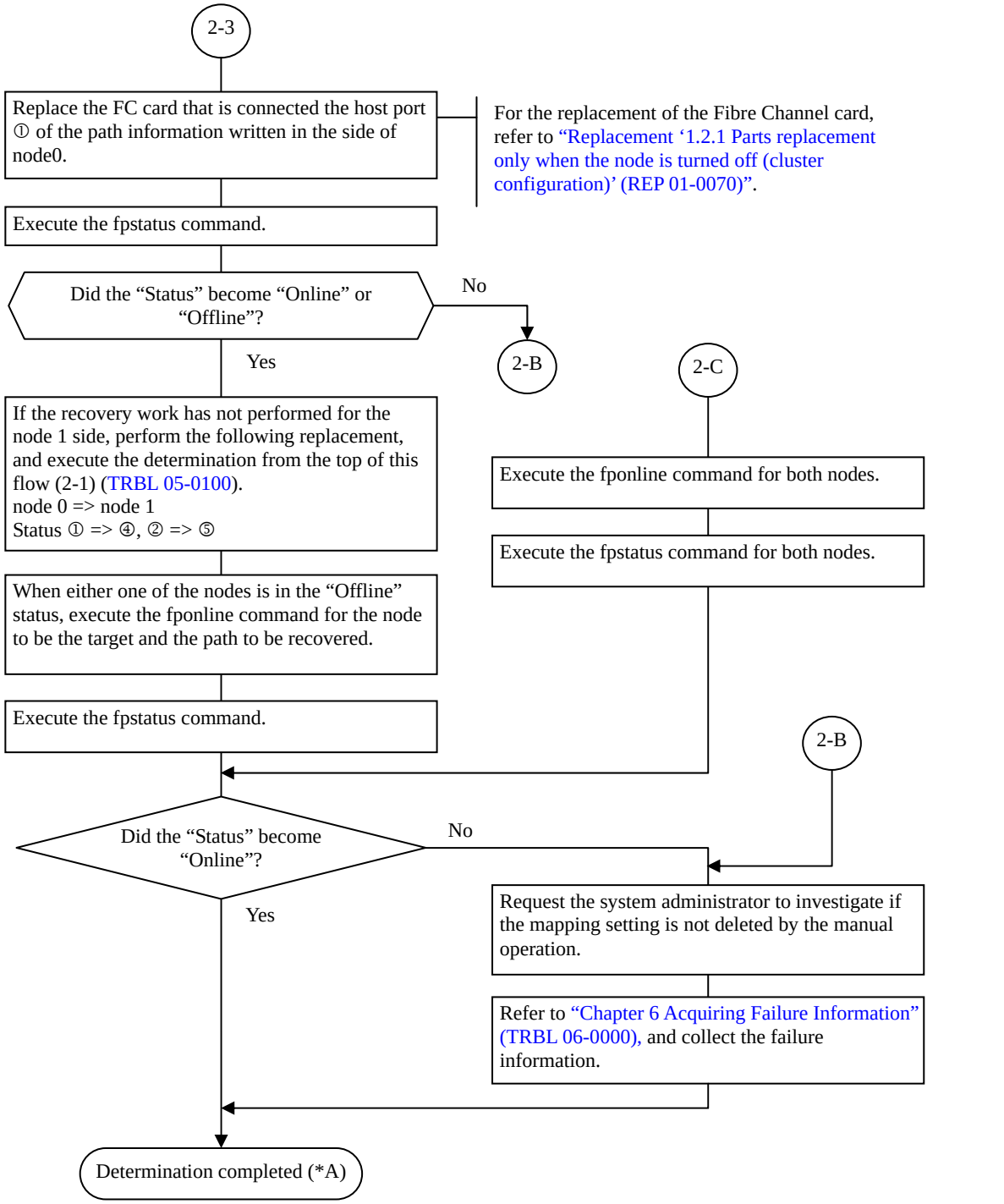
Path	Target	HostPort ④	HostPortWWN	ArrayPort ⑤	ArrayPortWWN	Model ⑥	Serial	Status
path000-0005-0B	N0-T000	fc0005	10000000c98f26ce	0B	50060e8005271c62	AMS	87010001	Error



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online", execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure at the cluster configuration".

Figure 5.1.2-2 Procedure 2 for Determining by FC Path Status (3/4)

Copyright © 2010, 2011, Hitachi, Ltd.



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online", execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure at the cluster configuration".

Figure 5.1.2-2 Procedure 2 for Determining by FC Path Status (4/4)

Copyright © 2010, 2011, Hitachi, Ltd.

(3) Determining failure recovery of case #3 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

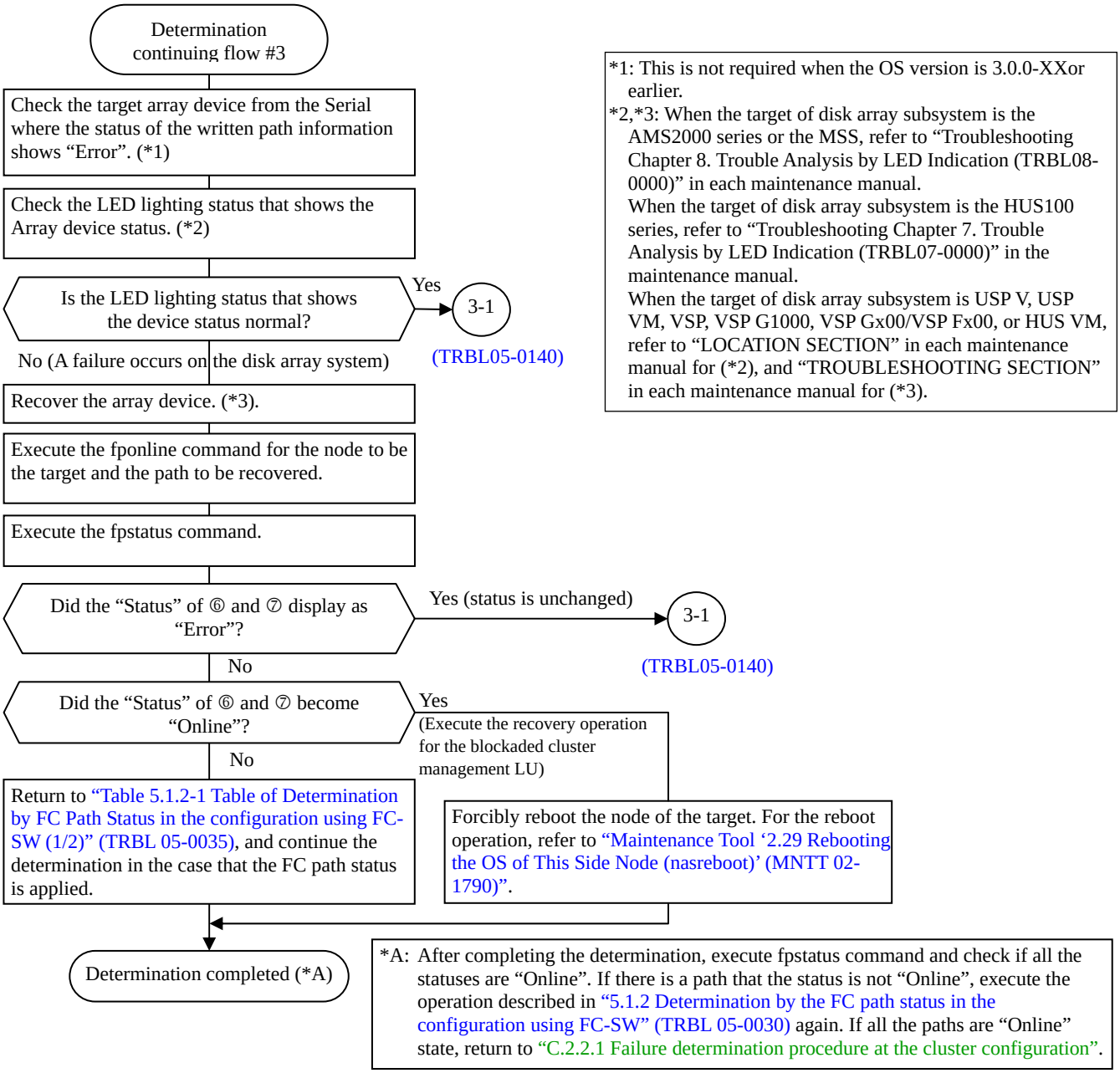


Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (1/7)

Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial ③	Status	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

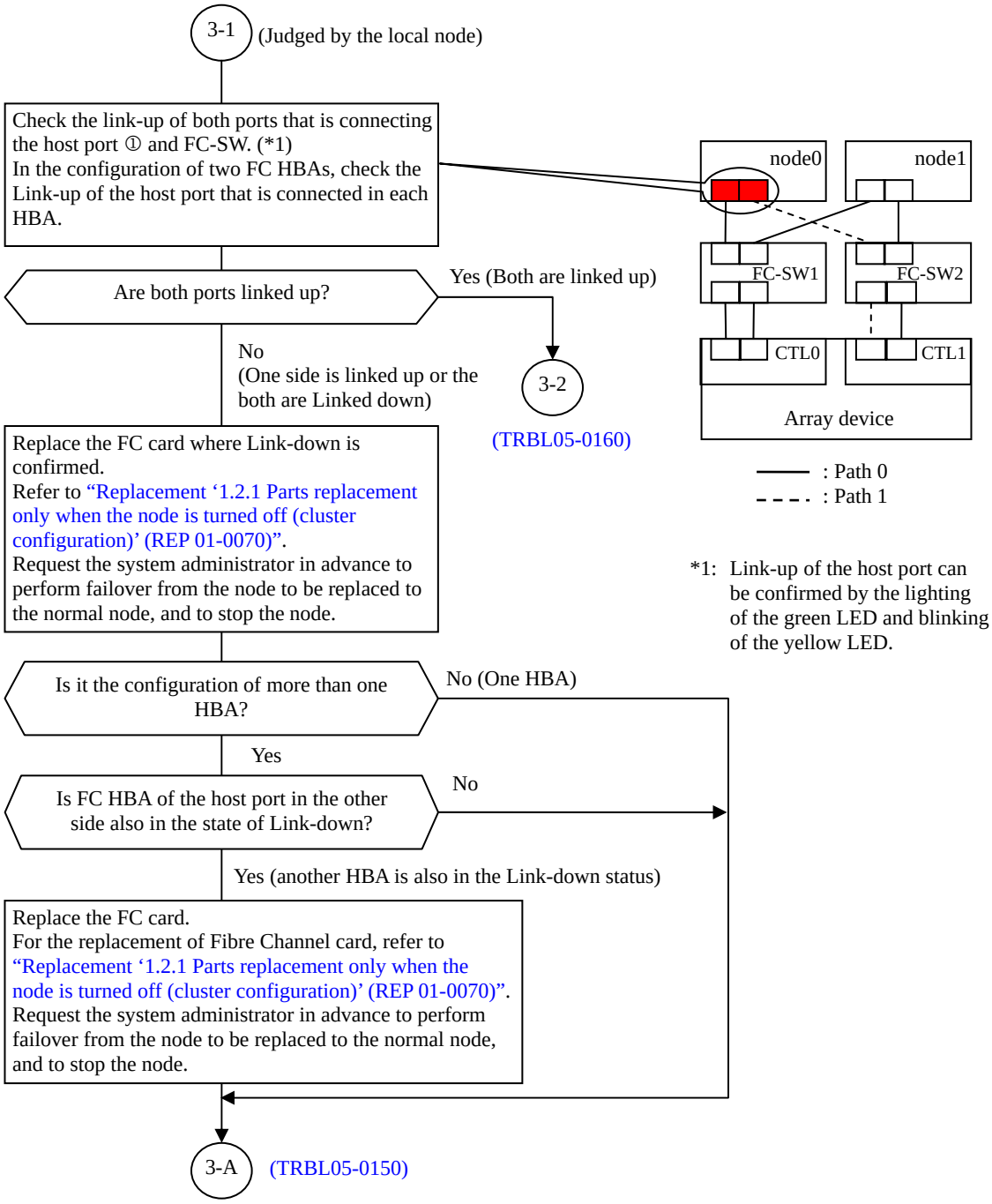


Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (2/7)

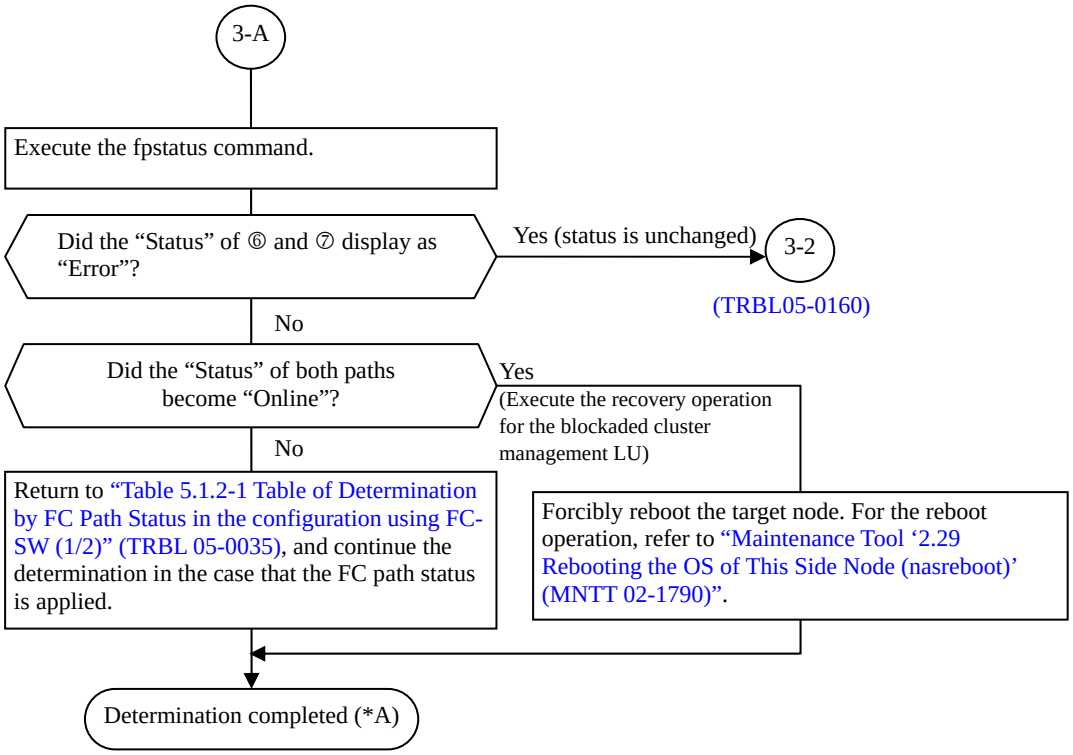
Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online", execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure at the cluster configuration".

Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (3/7)

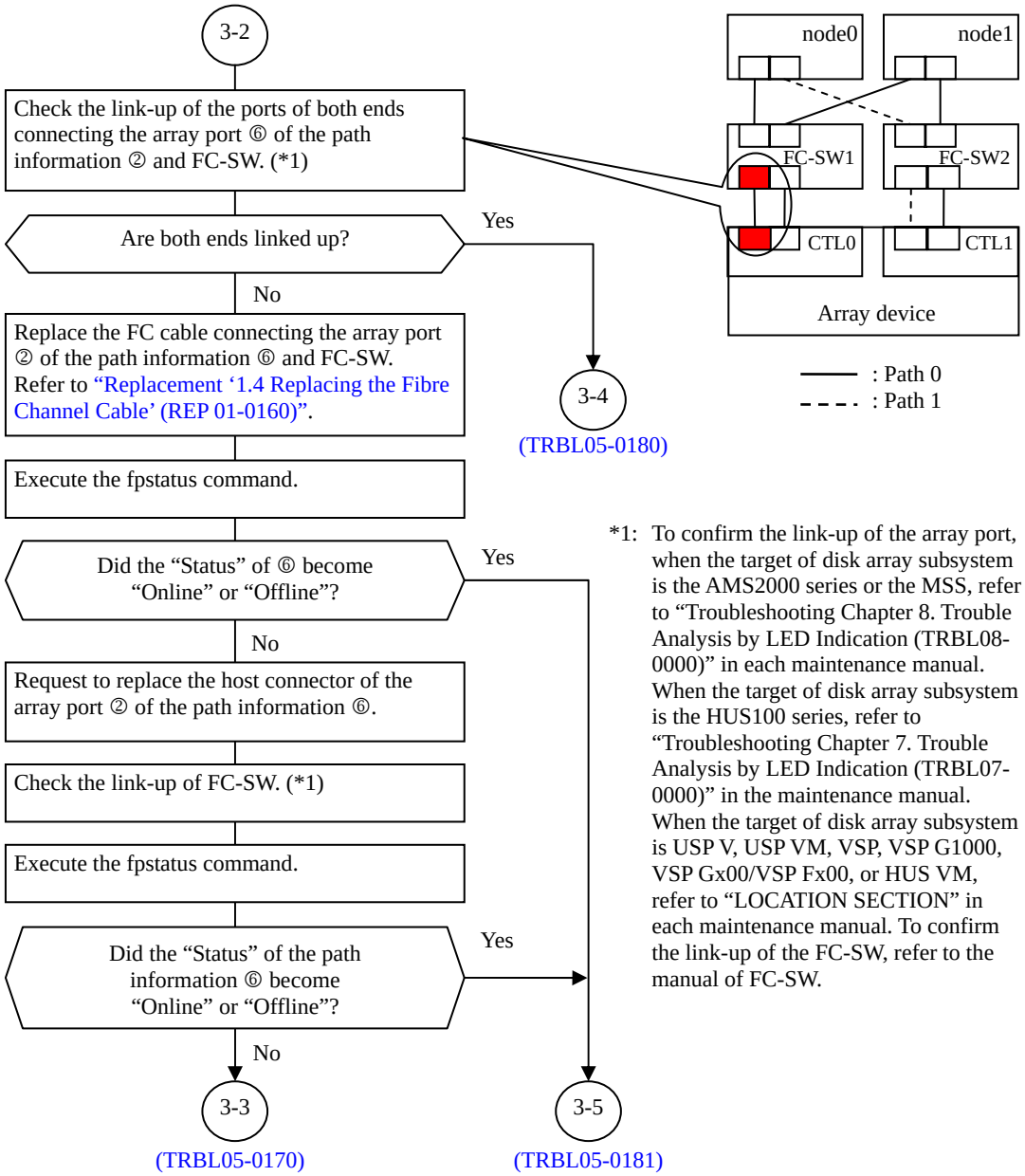
Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*1: To confirm the link-up of the array port, when the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual. When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual. When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual. To confirm the link-up of the FC-SW, refer to the manual of FC-SW.

Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (4/7)

Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN	ArrayPort ⑤	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

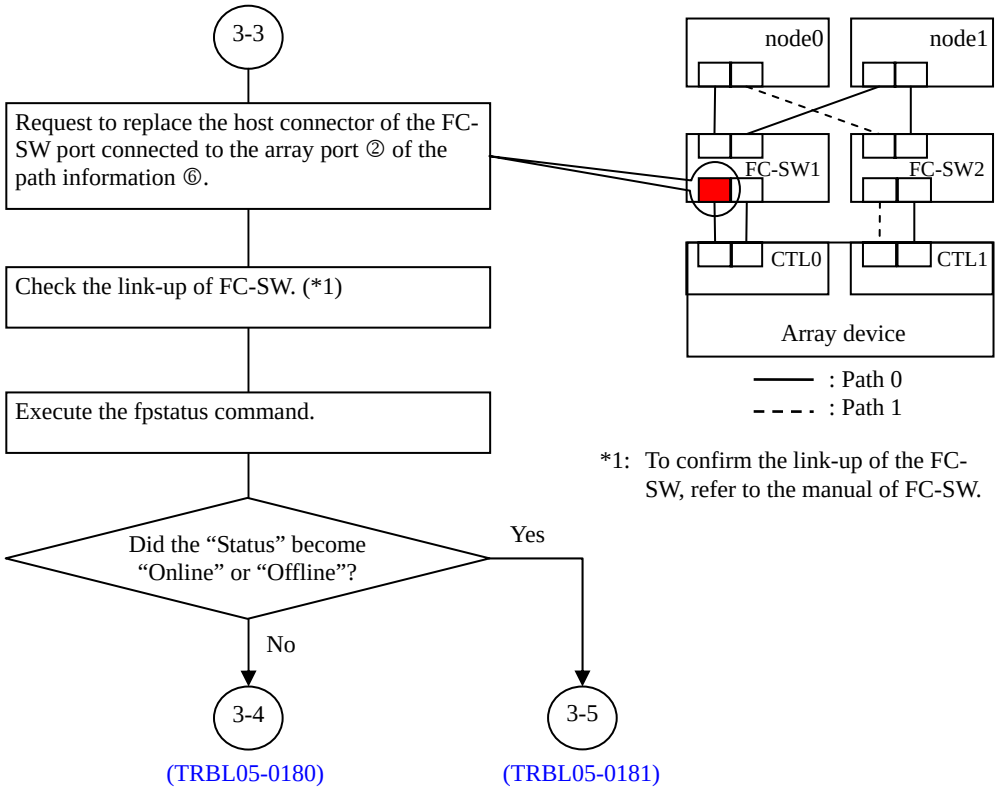


Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (5/7)

Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

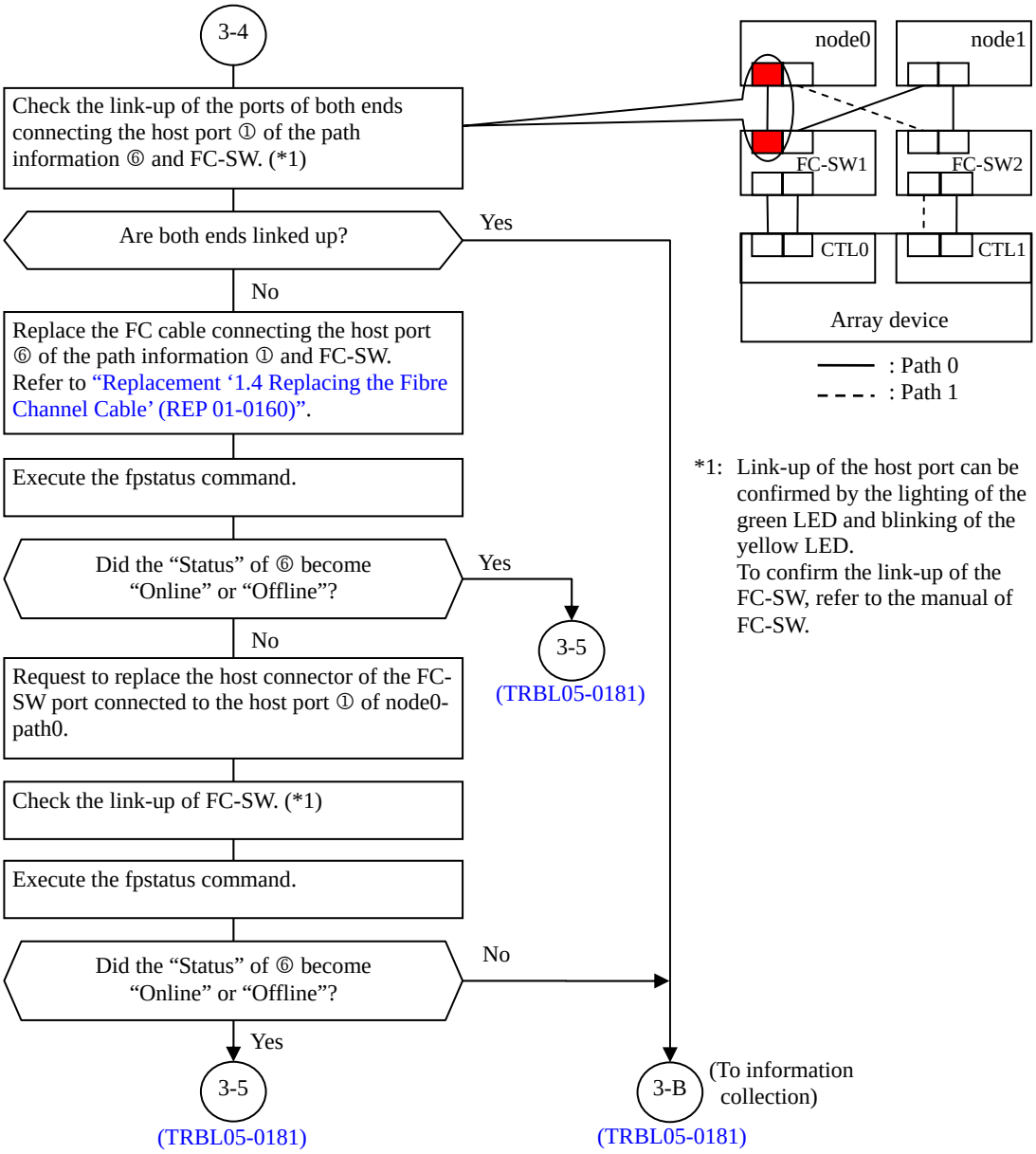


Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (6/7)

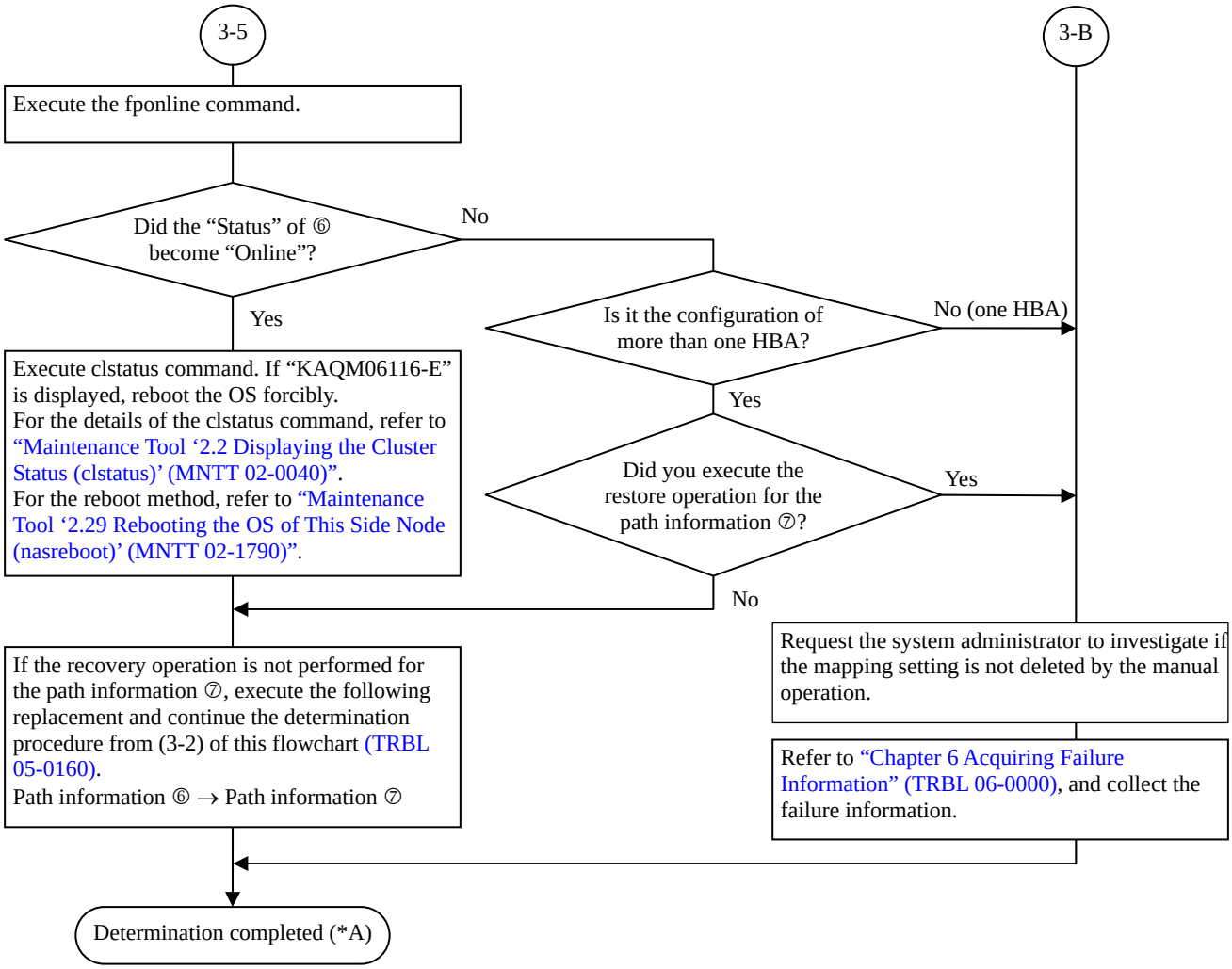
Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online", execute the operation described in "5.1.2 Determination by the FC path status in the configuration using FC-SW" (TRBL 05-0030) again".
If all the paths are "Online" state, return to "C.2.2.1 Failure determination procedure at the cluster configuration".

Figure 5.1.2-3 Procedure 3 for Determining to the FC Path Status (7/7)

Copyright © 2011, Hitachi, Ltd.

(4) This page is intentionally blanked.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

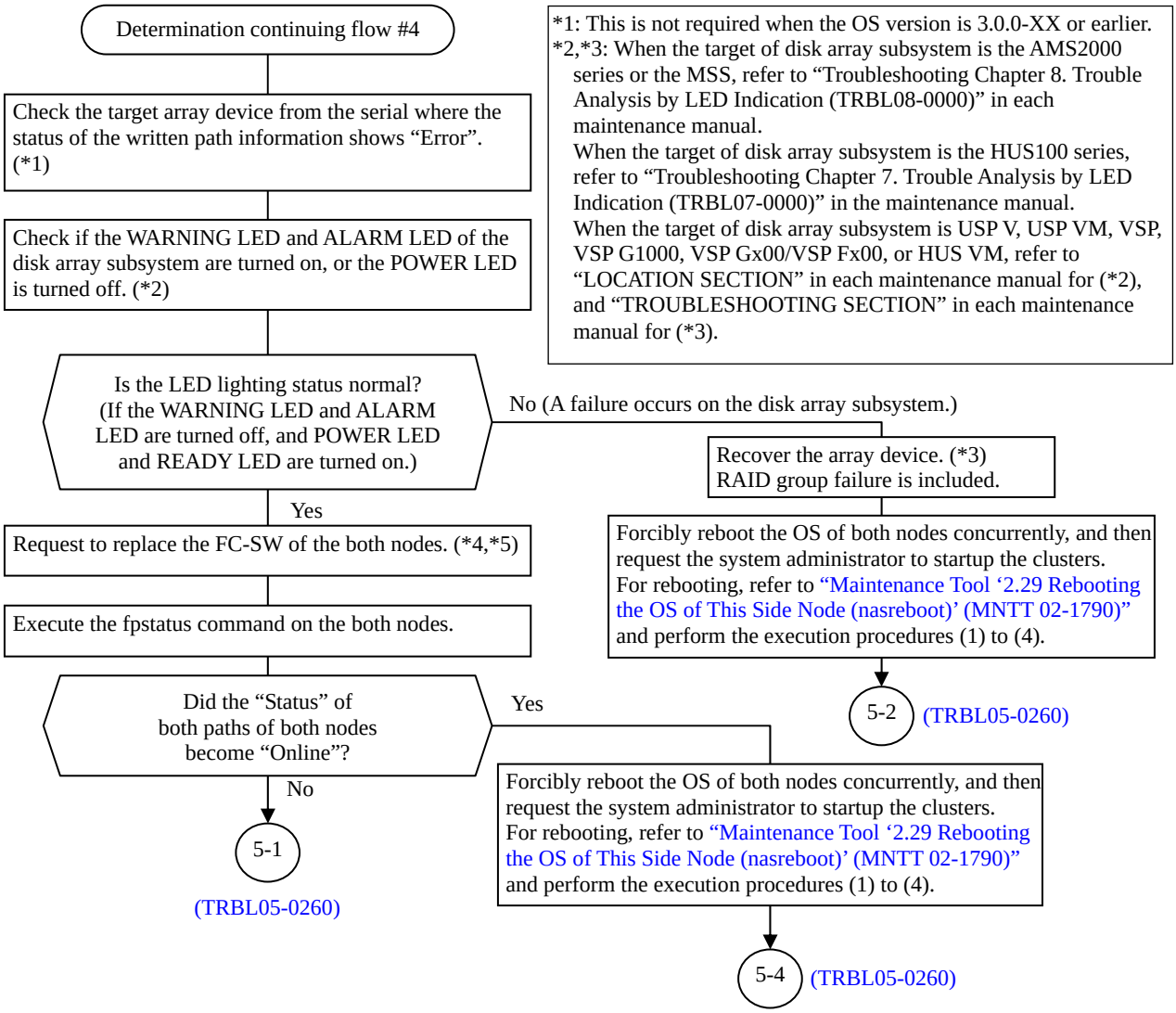
(5) Determining failure recovery of case #4 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑤	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ③	HostPortWWN ④	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑥
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Error
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Error



*1: This is not required when the OS version is 3.0.0-XX or earlier.
*2,*3: When the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual.
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual for (*2), and "TROUBLESHOOTING SECTION" in each maintenance manual for (*3).

*4: Request the system administrator to write down all of the zoning information in advance, because the WWN zoning might be necessary to be set again after the replacement of FC-SW.
*5: In the configuration of HDI for HCP, request the system administrator for planned stopping of the HCP before replacing FC-SW, then start up the HCP after completing the FC-SW replacement.

Figure 5.1.2-5 Procedure 5 for Determining to the FC Path Status (1/2)

Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑤	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ③	HostPortWWN ④	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑥
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Error
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Error

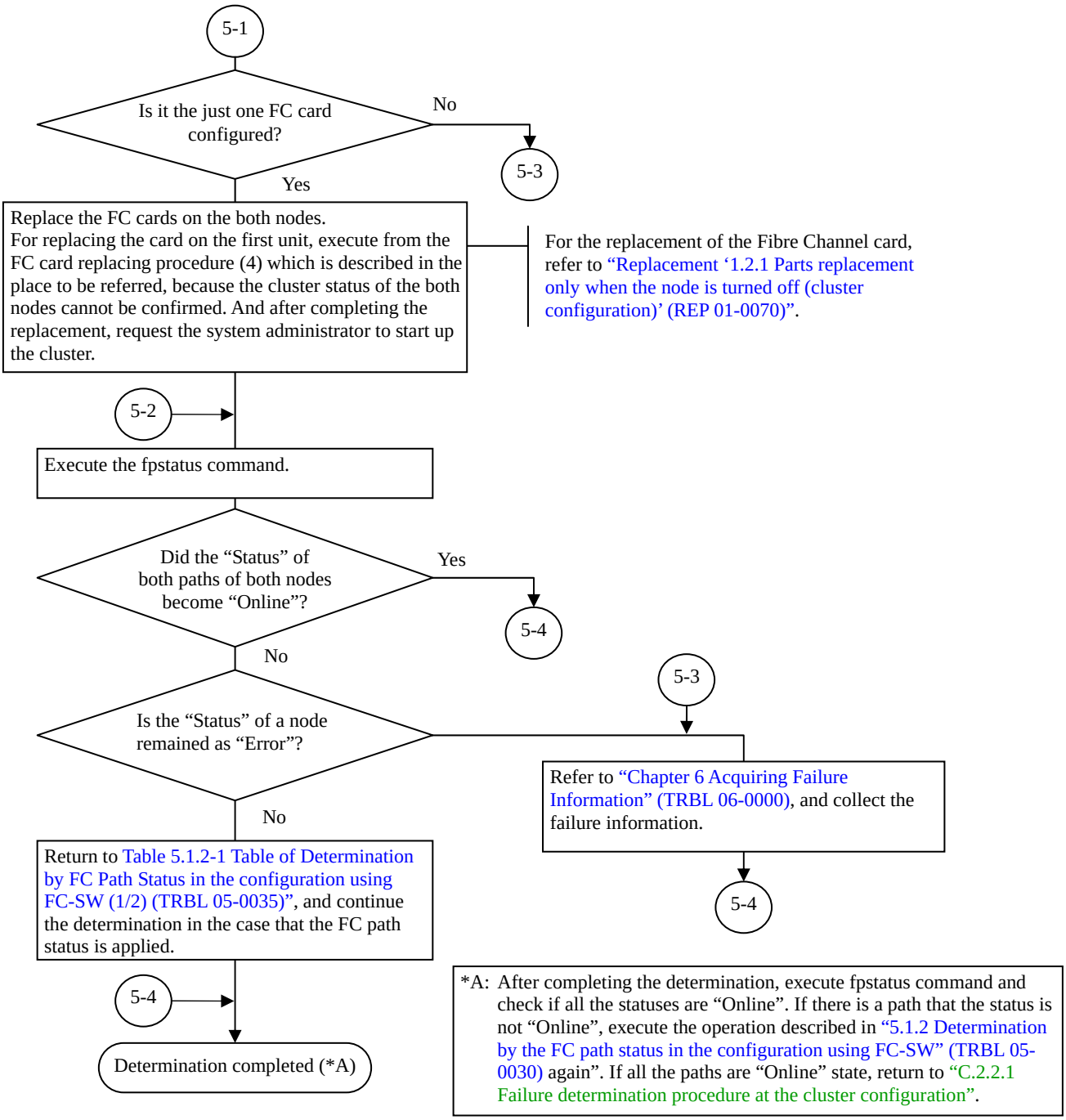


Figure 5.1.2-5 Procedure 5 for Determining to the FC Path Status (2/2)

Copyright © 2010, 2011, Hitachi, Ltd.

(6) Determining failure recovery of case #5 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③
-	-	fc0004	10000000c98f26be	0A	50060e8005271c62		87010001	Unknown
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

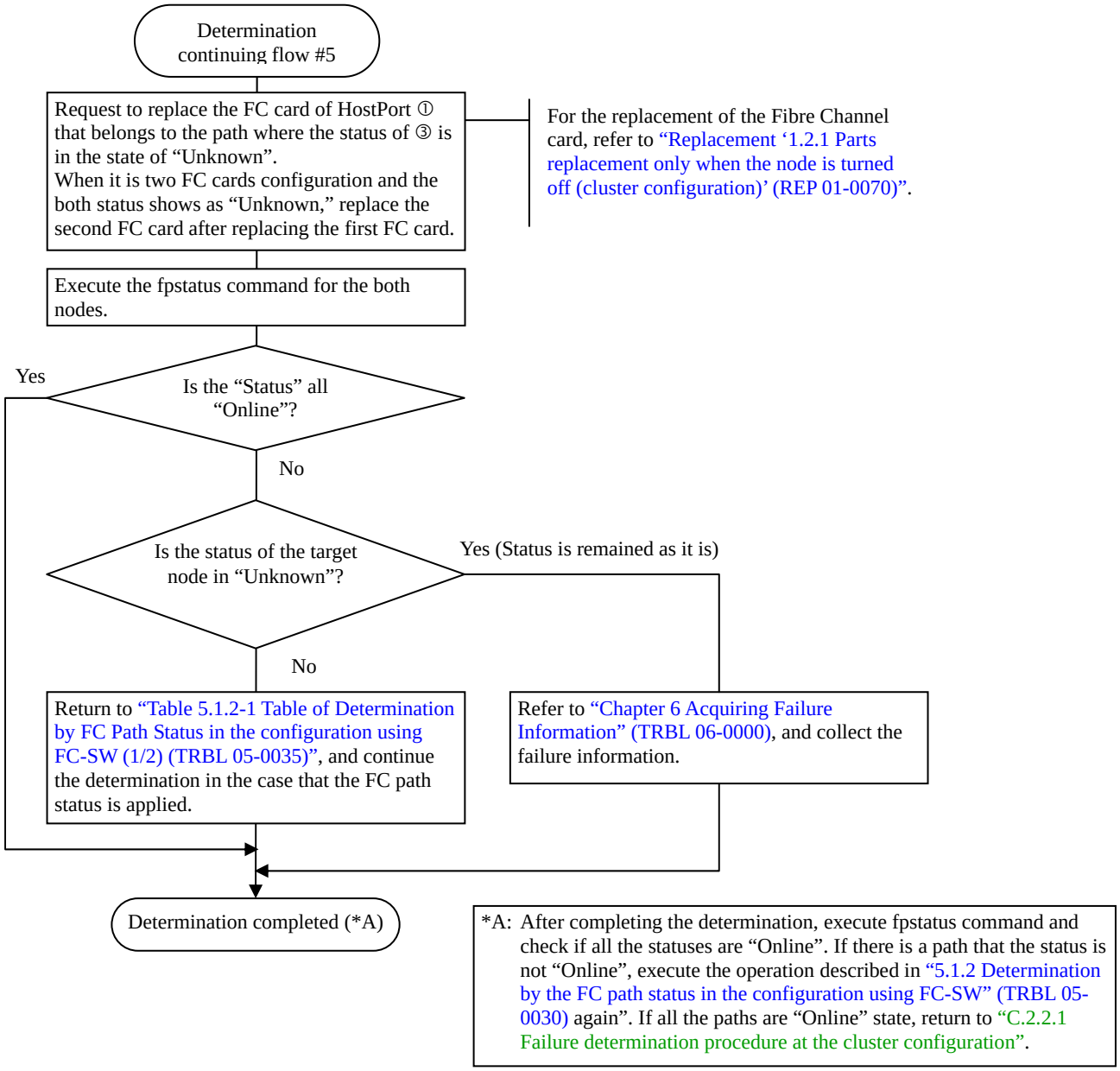


Figure 5.1.2-6 Procedure 6 for Determining to the FC Path Status

Copyright © 2010, 2011, Hitachi, Ltd.

(7) Determining failure recovery of case #6 in the table of determination
When the FC path status includes “Configuration Mismatch”, operation errors (setting errors at the time of adding the zoning or mapping, or fpstatus command is executed after rebooting OS) are considered. Therefore, perform the following.

Refer to (a) when the OS version is 2.2.1-XX or earlier, and refer to (b) when the OS version is 3.0.0-XX or later. For the confirmation of the OS version, refer to “Maintenance Tool ‘2.34 Displaying the Version of the OS (versionlist)’ (MNTT 02-2060)”.

(a) When the OS version is 2.2.1-XX or earlier

(a-1) When the FC path status is " Configuration Mismatch " for both in the path0 and path1 as below:

```
$ sudo fpstatus
Path              Target     HostPort HostPortWWN       ArrayPort  ArrayPortWWN      Status
path000-0004-0A N0-T000  fc0004   10000000c98f26be  0A         50060e800044b632  Configuration Mismatch
path000-0005-1B N0-T000  fc0005   10000000c98f36be  1B         50060e800044b634  Configuration Mismatch
```

FC path status after fpstatus command execution	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch	Request the system administrator to check if there is no error in operation (such as setting errors at the time of adding the zoning or mapping).

(a-1) When the FC path status is "Configuration Mismatch" either in the path0 or in the path1, and nothing is displayed in the other one as below:

```
$ sudo fpstatus
Path              Target     HostPort HostPortWWN       ArrayPort  ArrayPortWWN      Status
path000-0004-0A N0-T000  fc0004   5000087000302100  0A         50060e800044b632  Configuration Mismatch
```

FC path status after fpstatus command execution	Action to be taken	
Path0 : Configuration Mismatch Path1 : No display	→ Path0 : Online Path1 : Error	Regarded as path 0= “Online” and path1 = “Error” as the description in the left, and determine with the “Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)” (TRBL 05-0035).

Copyright © 2010, 2014, Hitachi, Ltd.

(b) When the OS version is 3.0.0-XX or later

(b-1) When the path0 and the path1 of the FC path status are “Configuration Mismatch” and the value of “Serial” and “Target” are the same as shown in the following.

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path000-0005-1B   N0-T000  fc0005    10000000c98f36be  1B        50060e800044b634  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (the values in Serial and Target are the same)	Execute “fpstatus--lipath” command, and check if there is a LU that does not have a replacing path. If there is such LU, request the system administrator to map the subject of LU. If there is no such LU, request the system administrator to confirm if there is any miss operation (setting failure on zoning and so on). For the details of fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

(b-2) When the path0 and the path1 of the FC path status are “Configuration Mismatch” and the value of “Serial” is the same but the value of “Target” is different (Four paths are displayed normally but only two paths are displayed by the failure.)

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path001-0005-1B   N0-T001  fc0005    10000000c98f36be  1B        50060e800044b634  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (The value of Serial is the same but the value of Target is different.)	Troubleshooting “Figure 5.1.2-7 Determination procedures by the FC path status 7” (TRBL05-0283)

Copyright © 2011, 2012, Hitachi, Ltd.

(b-3) The path0 and the path1 of the FC path status are “Configuration Mismatch,” but the value of “Serial” and “Target” are different (in the case of multi array configuration)

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path001-0005-0A   N0-T001  fc0005    10000000c98f36be  0A        50060e800044b366  AMS   87010010   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (The value of “Serial” and “Target” are different.)	Execute the corresponding contents described in (b-4) for each Serial and Target.

(b-4) As described in the following, either one of the path0 and path1 of the FC path status is “Configuration Mismatch,” and the other side FC path status is not displayed. (Two paths are normally displayed, but only one path is displayed as below due to a failure.)

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken	
Path0 : Configuration Mismatch Path1 : No display	→ Path0 : Online Path1 : Error	Assume path0 = “Online”, and path1= “Error” as shown in the description in the left, and then determine in reference to Table 5.1.2-1 Table of Determination by FC Path Status in the configuration using FC-SW (1/2)” (TRBL 05-0035).

Copyright © 2011, Hitachi, Ltd.

node0

Path	Target	HostPort	HostPortWWN	① ArrayPort	ArrayPortWWN	Model	② Serial	③ Status
path000-0004-0A	N0-T000	fc0004	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch
path001-0005-1B	N0-T001	fc0005	10000000c98f56be	1A	50060e8005238b64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort	HostPortWWN	④ ArrayPort	ArrayPortWWN	Model	⑤ Serial	⑥ Status
path000-0006-1A	N1-T000	fc0006	10000000c98f56be	1A	50060e8005238b64	AMS	87010001	Configuration Mismatch
path001-0007-1B	N1-T001	fc0007	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch

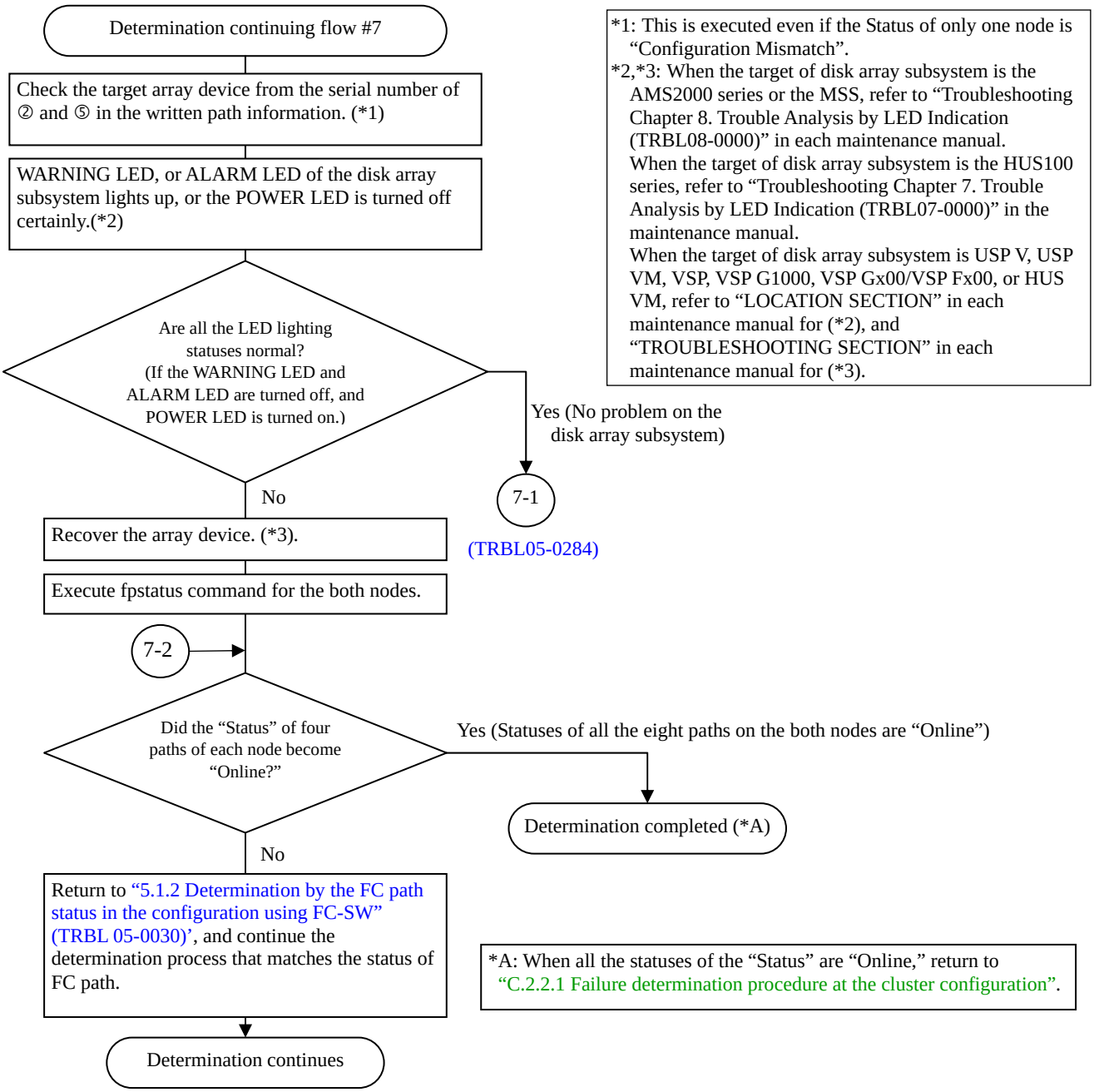


Figure 5.1.2-7 Determination procedures by the FC path status 7 (1/2)

Copyright © 2011, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort	HostPortWWN	① ArrayPort	ArrayPortWWN	Model	② Serial	③ Status
path000-0004-0A	N0-T000	fc0004	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch
path001-0005-1B	N0-T001	fc0005	10000000c98f56be	1A	50060e8005238b64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort	HostPortWWN	④ ArrayPort	ArrayPortWWN	Model	⑤ Serial	⑥ Status
path000-0006-1A	N1-T000	fc0006	10000000c98f56be	1A	50060e8005238b64	AMS	87010001	Configuration Mismatch
path001-0007-1B	N1-T001	fc0007	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch

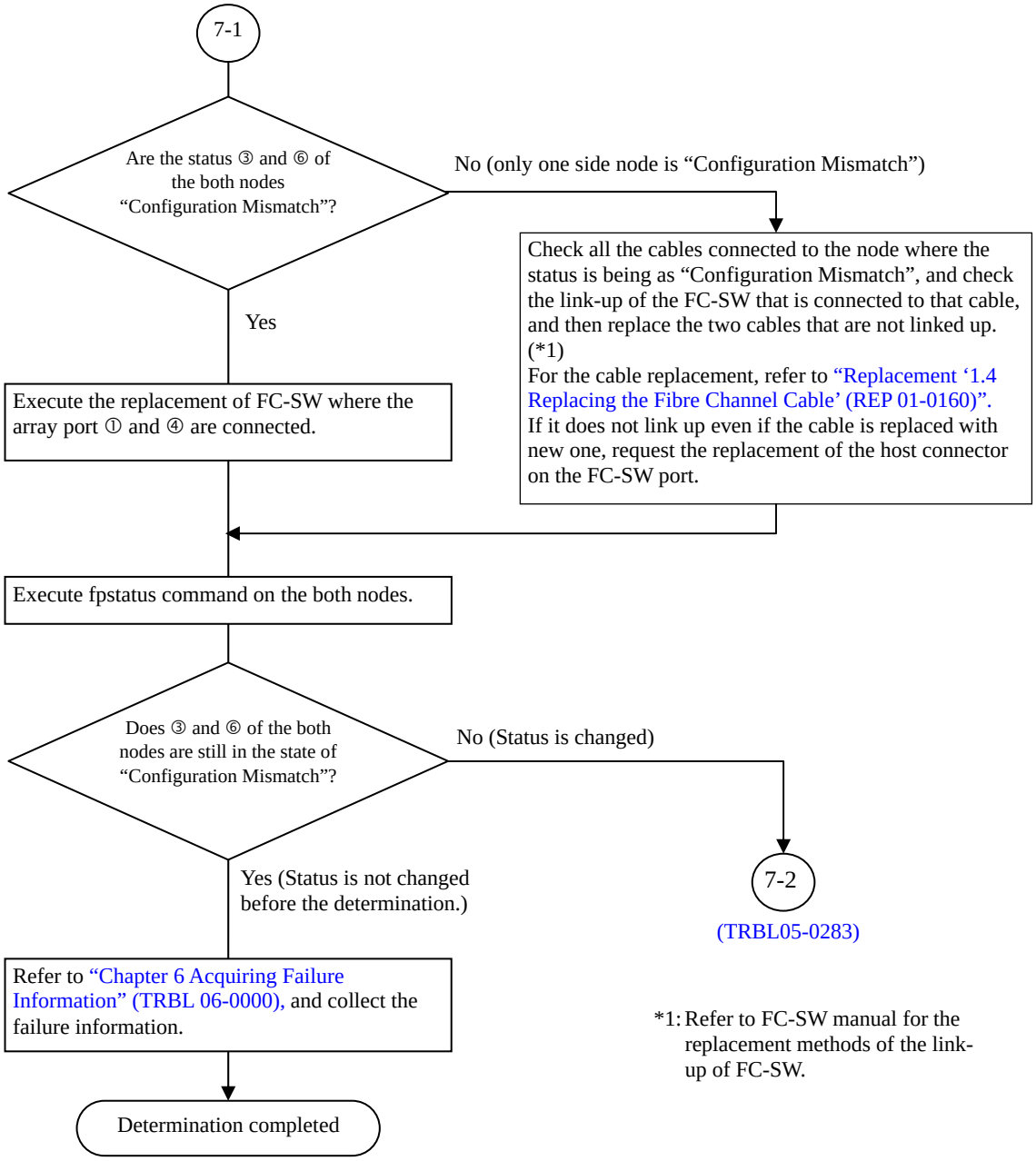


Figure 5.1.2-7 Determination procedures by the FC path status 7 (2/2)

Copyright © 2011, Hitachi, Ltd.

(8) Determining failure recovery of case #7 in the table of determination
When the FC path status has “Offline” or “Partially Online”, forgetting the procedure after the manual operation is considered. Perform the following.

① Request the system administrator to execute the fponline command for the relevant FC path and change the FC path status to “Online”. Refer to “Maintenance Tool ‘2.9 Switching the FC Path to Online (fponline)’ (MNTT 02-0590)”.
② After completing determination, return to “C.2.2 Determination Procedure when a Failure Occurred”.

(9) Determining failure recovery of case #8 in the table of determination
When it is not applied to any cases in the table of determination, a disk array defect or a dual failure of the device may have occurred or the FC path failure may be recovered.
Execute (9-1) in the case of the cluster configuration and all of the FC path status are “Online”, otherwise execute (9-2.)

(9-1) In the case all of the FC path status are “Online”
① Execute the clstatus command. For the details of the clstatus command, refer to “Maintenance Tool ‘2.2 Displaying the Cluster Status (clstatus)’ (MNTT 02-0040)”.

② Execute ③ if the error message “KAQM06116-E” was displayed as the execution result, otherwise execute (9-2).

③ Reboot the OS of both nodes forcibly because the cluster management LU is blocked. For the reboot operation, refer to “Maintenance Tool ‘2.29 Rebooting the OS of This Side Node (nasreboot)’ (MNTT 02-1790)” and perform the execution procedures (1) to (4).

④ After completing the operation above, return to “C.2.2 Determination Procedure when a Failure Occurred”.

(9-2) In the case of other than (9-1)
① Refer to Troubleshooting “Chapter 6 Acquiring Failure Information” (TRBL 06-0000), and collect the failure information.

② After collecting the information, contact the support center and follow the instructions.

③ After completing determination, return to “C.2.2 Determination Procedure when a Failure Occurred”.

Copyright © 2010, 2014, Hitachi, Ltd.

5.1.3 Determination by the FC path status in the configuration without using FC-SW

Based on the written path information, determine the failure in "Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)" (TRBL 05-0305) as shown below.

In the cluster configuration, if all the ports are used in the configuration with two FC-cards, the four paths in each node are displayed as shown in the following examples. In this case, consider the replacing path that refers to the same LU in each node as one combination, and determine the failure from the path statuses shown in "Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)" (TRBL 05-0305). If four paths are displayed in each node, determination process must be done for each replacing path.
The paths to be replaced are the two paths that match the "Serial" and "Target" as shown in the following execution example in each node. (In the execution example in the next page, it is "N0-T000" and "N0-T001" in node0, and "N1-T000" and "N1-T001" in node1.)

There is another replacing path that refers to the same LU in the other side node. In the following examples, ① and ② are the combination of the replacing path that refers to the same LU.

However, when the path status is "Unknown" or "Configuration Mismatch," all the path status will not be displayed, or "Target" and "Serial" are not displayed. Therefore, when the path status is "Unknown" or "Configuration Mismatch," follow the instruction described in Troubleshooting "Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (2/2)" (TRBL 05-0310).

Copyright © 2010, 2012, Hitachi, Ltd.

- Execution example when all the ports are used in the configuration of two FC cards.

[Connected four paths in the same array]

Execution example of node0

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
① path000-0004-0A   N0-T000  fc0004   10000000c98f26be 0A        50060e800044b632  AMS   87010001   Online
  path000-0006-1C   N0-T000  fc0006   10000000c98f36be 1C        50060e800044b636  AMS   87010001   Error
  path001-0005-0B   N0-T001  fc0005   10000000c98f36ce 0B        50060e8005271c72  AMS   87010001   Online
  path001-0007-1D   N0-T001  fc0007   10000000c98f48ae 1D        50060e8005271c76  AMS   87010001   Online
```

Execution example of node1

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
② path000-0004-1A   N1-T000  fc0004   10000000c98f27ab 1A        50060e800044b666  AMS   87010001   Online
  path000-0006-0C   N1-T000  fc0006   10000000c98f37bc 0C        50060e800044b682  AMS   87010001   Online
  path001-0005-1B   N1-T001  fc0005   10000000c98f46cb 1B        50060e8005271b76  AMS   87010001   Error
  path001-0007-0D   N1-T001  fc0007   10000000c98f52ac 0D        50060e8005271a72  AMS   87010001   Online
```

[In the multi array configuration]

Execution example of node0

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
① path000-0004-0A   N0-T000  fc0004   10000000c98f26be 0A        50060e8005271c62  AMS   87010001   Online
  path000-0006-1C   N0-T000  fc0006   10000000c98f36be 1C        50060e8005271c60  AMS   87010001   Error
  path001-0004-0B   N0-T001  fc0004   10000000c98f46ce 0B        50060e8005238f42  AMS   87010010   Online
  path001-0006-1D   N0-T001  fc0006   10000000c98f52ae 1D        50060e8005238f64  AMS   87010010   Online
```

Execution example of node1

```
$ sudo fpstatus - v
Path                Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
② path000-0004-1A   N1-T000  fc0004   10000000c98f27ab 1A        50060e8005271c60  AMS   87010001   Online
  path000-0006-0C   N1-T000  fc0006   10000000c98f37bc 0C        50060e8005271c62  AMS   87010001   Online
  path001-0004-1B   N1-T001  fc0004   10000000c98f46cb 1B        50060e8005272a82  AMS   87010010   Error
  path001-0006-0D   N1-T001  fc0006   10000000c98f52ac 0D        50060e8005272a86  AMS   87010010   Online
```

When the OS version is 3.0.0-XX or later, specifying "--allnode" to fpstatus command can refer to the path information of the both nodes. However, when the communication cannot be done with the other side node, the information of the other side node may not be displayed. In this case, specify "-v" option to fpstatus in each node, and refer to the both nodes information. For the confirmation of the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".
For the details about fpstatus command, refer to "Maintenance Tool '2.5 Displaying the FC Status (fpstatus)' (MNTT 02-0280)".

The next page shows the identifying method of the combination of paths when the four or more FC path information excepting "Unknown" and "Configuration Mismatch" are displayed as shown in the above path information.

Copyright © 2011, 2012, Hitachi, Ltd.

In the determination table shown in Troubleshooting “Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)” (TRBL 05-0305), determination is done by using a combination of the path information that refers to the same LU between the target node and the other side node. Therefore, it is required to identify the path information that refers to the same LU in each node or that refers to the same LU between the nodes.
The method of identifying the path information that refers to the same LU is described below when the fpstatus execution example of each node are the following.

Execution example of node0

```
$ sudo fpstatus - v
Path                 Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
① path000-0004-0A    N0-T000  fc0004   10000000c98f26be 0A        50060e800044b632 AMS   87010001 Online
  path000-0006-1C    N0-T000  fc0006   10000000c98f36be 1C        50060e800044b636 AMS   87010001 Error
  path001-0005-0B    N0-T001  fc0005   10000000c98f36ce 0B        50060e8005271c72 AMS   87010001 Online
  path001-0007-1D    N0-T001  fc0007   10000000c98f48ae 1D        50060e8005271c76 AMS   87010001 Online
```

Execution example of node1

```
$ sudo fpstatus - v
Path                 Target   HostPort HostPortWWN      ArrayPort ArrayPortWWN      Model Serial     Status
② path000-0004-1A    N1-T000  fc0004   10000000c98f27ab 1A        50060e800044b666 AMS   87010001 Online
  path000-0006-0C    N1-T000  fc0006   10000000c98f37bc 0C        50060e800044b682 AMS   87010001 Online
  path001-0005-1B    N1-T001  fc0005   10000000c98f46cb 1B        50060e8005271b76 AMS   87010001 Error
  path001-0007-0D    N1-T001  fc0007   10000000c98f52ac 0D        50060e8005271a72 AMS   87010001 Online
```

1. Verify the replacing path in each node. The replacing paths have the path information where “Target” is the same.
   On the above example, the first path is the path that contains “N0-T000” and the second path is the path that contains “N0-T001” in the node0. In the same manner, the first path is the path that contains “N1-T000” and the second path is the path that contains “N1-T001” in the node1.
2. Next, identify the path combination that refers to the same LU between the node0 and node1. [In the case of multi-array configuration] shown in “TRBL 05-0301,” four paths in each node are displayed but the “Serial” is different in each replacing part. Therefore, ① and ② that match the “Serial” in the both nodes can be identified that it refers to the same LU between the nodes. After the identification, proceed to step3.
   However, if “Serial” of the replacing path is the same as shown in the above example, it is needed to identify the path information that refers to the same LU with either method of the following.
   The first method is to execute fpstatus command with "--lupath" option. ((1) A method of using fpstatus command to identify the same LU between the nodes.)
   For fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.
   The second method is to identify with “Maintenance Tool ‘2.35 Displaying the LU Information in the Disk Array Subsystem (alulist)’ (MNTT 02-2090)”. ((2) A method of using alulist command to identify the path that refers to the same LU between the nodes.)
   The determination method is described from the next page.
3. Write down the FC path information of the both nodes that refer to the same LU identified at the step “2”.

Copyright © 2011, 2012, Hitachi, Ltd.

4. Based on the path that identified in the above description, execute the determination operation by confirming the FC path status of ① as the target node and of ② as the other side of the node from Troubleshooting “Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)” (TRBL 05-0305).
   In the execution example in the previous page, execute the determination process of #1 on the path0 and path1 of the target node is “Online” and “Error” respectively, and the path0 and path1on the other side node is “Online” and “Online” respectively.
5. After completing the step “4,” check the status of the other side replacing path, and if there is a path that the status is not in “Online”, execute the step “2” and “3”. In the execution example in the previous page, execute the determination procedure of #2 that the path0 and path1 on the target node is “Online” and “Error” respectively, and the path0 and path1 on the other side node is “Error” and “Online” respectively.

Copyright © 2011, Hitachi, Ltd.

(1) A method of using fpstatus command to identify the same LU between the nodes

Since this procedure cannot be done in 3.0.0-XX or earlier OS version, execute Troubleshooting "5.1.2 (2) A method of using alulist command to identify the path that refers to the same LU between the nodes" (TRBL 05-0034).

For the confirmation of the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".

(a) Execute "fpstatus --lupath" in either of the nodes. Figure 5.1.3-A is an execution example at the side of node0. The LU information of both nodes can be displayed. However, if the communication cannot be done with the other side node, the information of the other side node may not be displayed. In this case, execute the procedure described in Troubleshooting "5.1.3 (2) A method of using alulist command to identify the path that refers to the same LU between the nodes" (TRBL 05-0304).

```
$ sudo fpstatus –lupath
Model   Serial LDEV(  hex)  ArrayPort Target   HostPort  HostPortWWN      Status      Mismatch
AMS     87010001  11(  000B) 0A       N0-T000   fc0004    10000000c98f26be Online      -
AMS     87010001  11(  000B) 1C       N0-T000   fc0006    10000000c98f36be Offline(E)  (1) -
AMS     87010001  11(  000B) 1A       N1-T000   fc0004    10000000c98f27ab Online      -
AMS     87010001  11(  000B) 0C       N1-T000   fc0006    10000000c98f37bc Online      -
AMS     87010001  21(  0015) 0A       N0-T000   fc0004    10000000c98f26be Online      -
AMS     87010001  21(  0015) 1C       N0-T000   fc0006    10000000c98f36be Offline(E)      -
AMS     87010001  21(  0015) 1A       N1-T000   fc0004    10000000c98f27ab Online      -
AMS     87010001  21(  0015) 0C       N1-T000   fc0006    10000000c98f37bc Online      -
AMS     87010001  31(  001F) 0B       N0-T001   fc0005    10000000c98f36ce Online      -
AMS     87010001  31(  001F) 1D       N0-T001   fc0007    10000000c98f48ae Online      (2)
AMS     87010001  31(  001F) 1B       N1-T001   fc0005    10000000c98f46cb Offline(E)  -
AMS     87010001  31(  001F) 0D       N1-T001   fc0007    10000000c98f52ac Online      -
AMS     87010001  41(  0029) 0B       N0-T001   fc0005    10000000c98f36ce Online      -
AMS     87010001  41(  0029) 1D       N0-T001   fc0007    10000000c98f48ae Online      -
AMS     87010001  41(  0029) 1B       N1-T001   fc0005    10000000c98f46cb Offline(E)      -
AMS     87010001  41(  0029) 0D       N1-T001   fc0007    10000000c98f52ac Online      -
```

Figure 5.1.3-A fpstatus ExecutionExample

(b) The LU path information of the both nodes is sorted in the order of "Serial" and "LDEV" as shown above. As in the thick frames on the above figure, four path information that refer to the same "LDEV" are displayed.

Looking at (1) in the above figure, "N0-T000" and "N1-T000" shown in "Target" can be confirmed as the path that refer to the same LU.

In the same manner, when looking at (2) in the above figure, "N0-T001" and "N1-T001" shown in "Target" can be confirmed as the path that refer to the same LU.

(c) From the result of (b), the path information that refers to the same LU is the path information of ①that includes "N0-T000" and the path information of ② that includes "N1-T000" in the execution example as shown in "TRBL 05-0302".

In the same manner, the other path information (a pair of "N0-T001" and "N1-T001") can be identified.

After the identification, proceed to step 3.

Copyright © 2011, 2012, Hitachi, Ltd.

(2) A method of using alulist command to identify the path that refers to the same LU between the nodes

(a) Compare the result of alulist command in the both nodes. Figure 5.1.3-B shows an execution example on the side of node0, and Figure 5.1.3-C shows an execution example on the side of node1. In each node, the LU information of one side ArrayPort of the replacing path is displayed.

```
$ sudo alulist
model    serial      LDEV(  hex)  port  type   size
AMS      87010001     0(  0000)   0A    SATA   70.000GB
AMS      87010001     3(  0003)   0A    SATA   30.000GB
• • • •
AMS      87010001    20(  0014)   0B    SATA   20.000GB
AMS      87010001    22(  0016)   0B    SATA   20.000GB
```

Figure 5.1.3-B Execution example of alulist on node0

(1)

(2)

```
$ sudo alulist
model    serial      LDEV(  hex)  port  type   size
AMS      87010001     0(  0000)   0C    SATA   70.000GB
AMS      87010001     3(  0003)   0C    SATA   30.000GB
• • • •
AMS      87010001    20(  0014)   0D    SATA   20.000GB
AMS      87010001    22(  0016)   0D    SATA   20.000GB
```

Figure 5.1.3-C Execution example of alulist on node1

(b) Identify “port” that refers to the same “LDEV” in both nodes. In the above diagram, “0A” on the side of node0 and “1A” on the side of node1from the “port” that refers to “0” of “LDEV” that is enclosed in (1) can be identified the ArrayPort that refers to the same LU in each node. In the same manner, “0B” on the side of node0 and “0B” on the side of node1 from the “port” that refers to “20” of “LDEV” that is enclosed in (2) can be identified the ArrayPort that refers to the same LU in each node.

(c) Identifying the one side of ArrayPort that refers to the same LU between the nodes in the step (b) can identify a combination of replacing path.
The ArrayPort “0A” on the side of node0 that is identified at (b) is included in the thick frame ① of the replacing path of node0 from the execution example as described in “TRBL 05-0302”. And the replacing path of node1 to be paired with that is the thick frame ② of the replacing path that includes ArrayPort “0C” of the node 1 identified at (b).
With the above information, ①and ② in the execution example described in “TRBL 05-0302” can be identified as the path information that refers to the same LU.
In the same manner, the other side path information can be identified.
After the identification, proceed to step 3.

Copyright © 2011, 2014, Hitachi, Ltd.

Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)

#	FC path status after fpstatus command execution		Assumed failure	Determination continuing flow
	node to be the target	node on opposite side		
1 (*1)	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Online	A failure has occurred in any of FC card, FC port, FC cable, FC-SW port (at the time of FC-SW configuration) and array port.	To the flow in Figure 5.1.3-1 (TRBL05-0320)
	Path 0 : Online Path 1 : Error	Path 0 : Online Path 1 : Online		
	Path 0 : Error Path 1 : Online	－(*2)		
	Path 0 : Error Path 1 : Online	－(*2)		
2 (*1)	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Error	• A failure on the array controller side has occurred. • A dual failure of No.1 has occurred.	To the flow in Figure 5.1.3-2 (TRBL05-0350)
	Path 0 : Online Path 1 : Error	Path 0 : Error Path 1 : Online		
	Path 0 : Error Path 1 : Online	Path 0 : Error Path 1 : Online		
	Path 0 : Online Path 1 : Error	Path 0 : Online Path 1 : Error		
3	Path 0 : Error Path 1 : Error	Path 0 : Online Path 1 : Online	• A dual failure of No.1 of the local node has occurred. • An FC card failure of the local node has occurred.	To the flow in Figure 5.1.3-3 (TRBL05-0380)
	Path 0 : Error Path 1 : Online	－(*2)	• A FC card failure of the local node has occurred. • A dual failure of the Item No.1 of the local node has occurred. • A dual failure of the disk array subsystem power supply has occurred. • Operation error (array shutdown) • A simultaneous failure of the array controller 0/1 has occurred.	
If a FC path status other than the above #1 to #4 is displayed, determine a failure based on the written downed path information in reference to "Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW(2/2)" (TRBL 05-0310).				

*1: When one side status of the FC path is "Configuration Mismatch", and the other side state of the FC path is not displayed as described below, determine it as "Configuration Mismatch" = "Online", and "No display" = "Error". (This status is shown when the OS is restarted after the path failure.)

FC path status after fpstatus command execution			FC path status after fpstatus command execution	
node to be the target	node on opposite side		node to be the target	node on opposite side
Path 0 : No display Path 1 : Configuration Mismatch	Path 0 : Online Path 1 : Online	=	Path 0 : Error Path 1 : Online	Path 0 : Online Path 1 : Online

If this state occurs after replacing HBA, there might be a mistake in inputting the WWN in the setting of the host group security of the disk array subsystem. Check the setting on the side of the disk array subsystem. If the WWN setting is wrong, correct it, and reboot the node in which the WWN setting was wrong. For the reboot method, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".
If there is no problem on the setting of the disk array subsystem, go to the determination procedure.

*2: In the single node configuration, only the FC path status of the target node is displayed.

Copyright © 2011, 2012, Hitachi, Ltd.

Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (2/2)

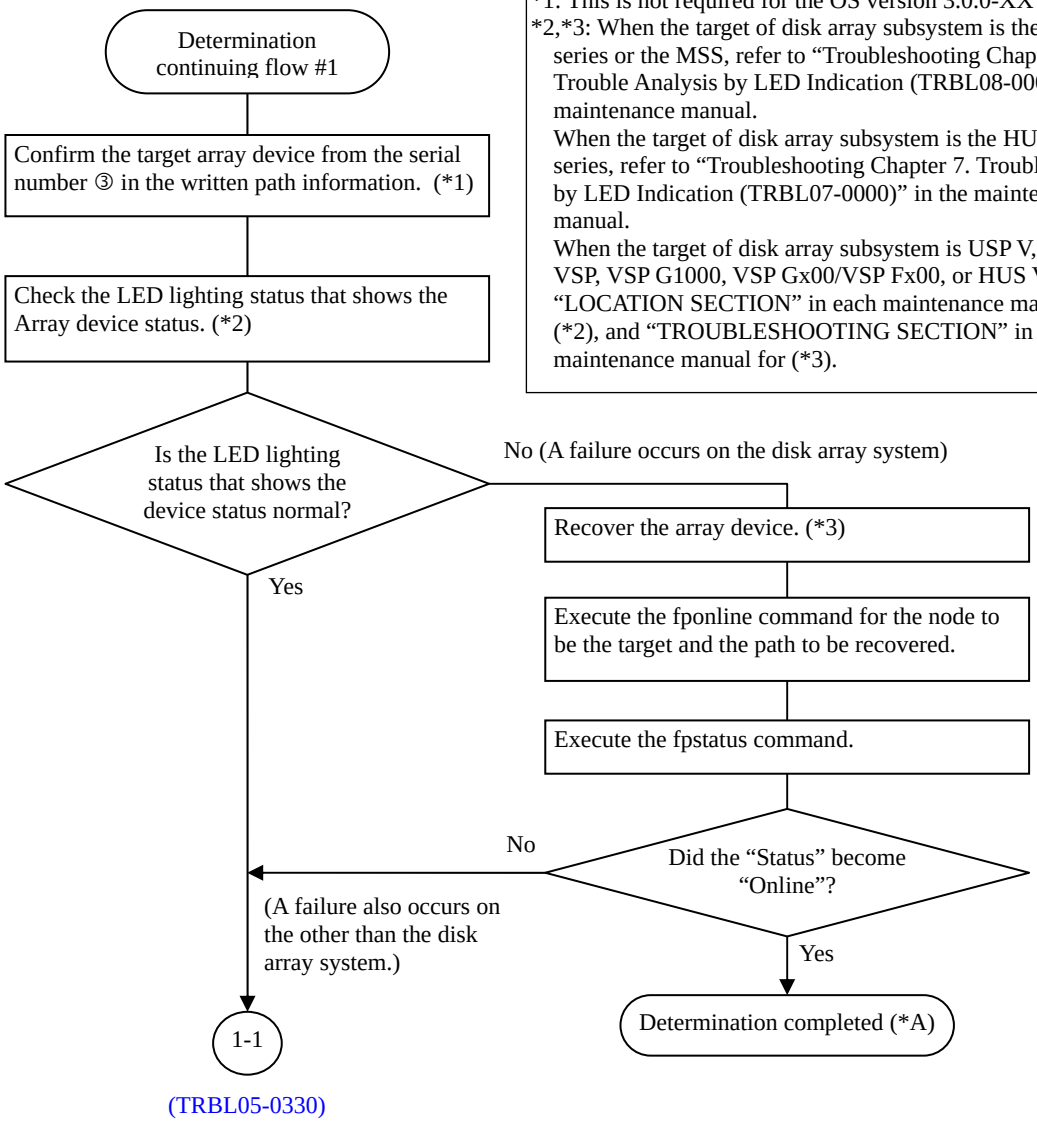
#	FC path status after fpstatus command execution		Assumed failure	Determination continuing flow
	node to be the target	node on opposite side		
4 (*3)	Path 0 : Error Path 1 : Error	Path 0 : Error Path 1 : Error	• A dual failure of No. 2 has occurred. • A dual failure of the array power supply has occurred. • Operation error (array shutdown) * Both nodes are restarted after the OSs down. Or, a dual failure of the array controller 0/1 has occurred.	To the flow in Figure 5.1.3-5 (TRBL05-0480)
5	Path 0 : Unknown Path 1 : Unknown	Path 0 : Online Path 1 : Online	An FC card failure has occurred.	(6) Determining failure recovery of case #5 in the table of determination (TRBL05-0490)
6	"Configuration Mismatch" is included (However, execute #5 when "Unknown" is included.)		• Operation error (setting error at the time of adding zoning or mapping) • Executed fpstatus command after the OS reboot when the path failure occurred.	(7) Determining failure recovery of case #6 in the table of determination (TRBL05-0500)
7	"Offline" or "Partially Online" exists		Forgetting the procedure after the manual operation and others	(8) Determining failure recovery of case #7 in the table of determination (TRBL05-0510)
8	Combination other than that		The disk array trouble or the dual failure of the device has occurred. Or the FC path failure is recovered.	(9)Determining failure recovery of case #8 in the table of determination (TRBL05-0510)

*3: If this state occurs after replacing HBA, there might be a mistake in inputting the WWN in the setting of the host group security of the disk array subsystem. Check the setting on the side of the disk array subsystem.
If the WWN setting is wrong, correct it, and reboot the node in which the WWN setting was wrong. For the reboot method, refer to "Maintenance Tool '2.29 Rebooting the OS of This Side Node (nasreboot)' (MNTT 02-1790)".
If there is no problem on the setting of the disk array subsystem, go to the determination procedure.

Copyright © 2010, 2014, Hitachi, Ltd.

(1) Determining failure recovery of case #1 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error



*1: This is not required for the OS version 3.0.0-XX or earlier.
*2,*3: When the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual.
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual for (*2), and "TROUBLESHOOTING SECTION" in each maintenance manual for (*3).

*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300)" again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-1 Procedure 1 for Determining by FC Path Status (1/3)

Copyright © 2010, 2016, Hitachi, Ltd.

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model	Serial ③	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

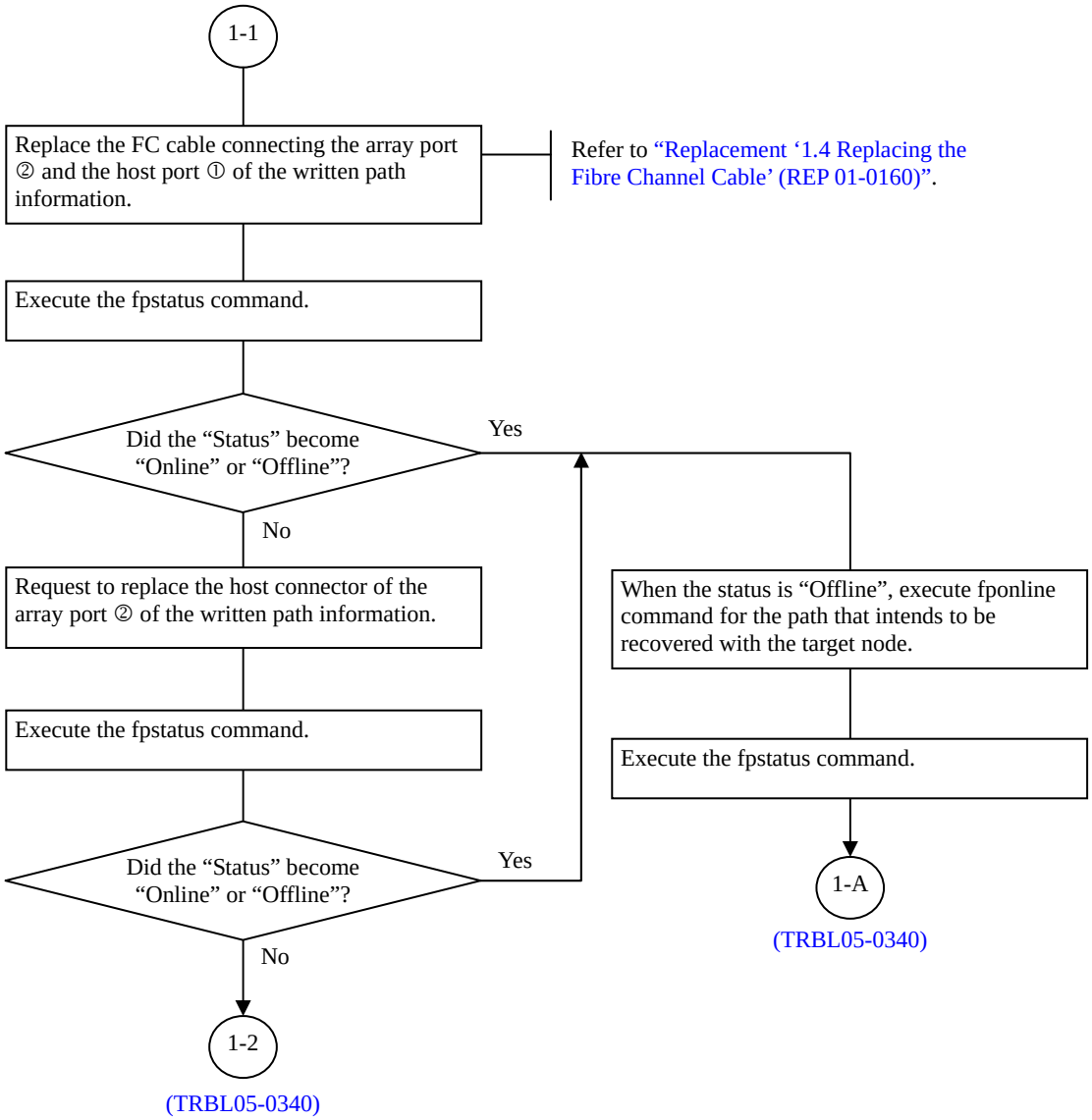


Figure 5.1.3-1 Procedure 1 for Determining by FC Path Status (2/3)

Copyright © 2010, 2014, Hitachi, Ltd.

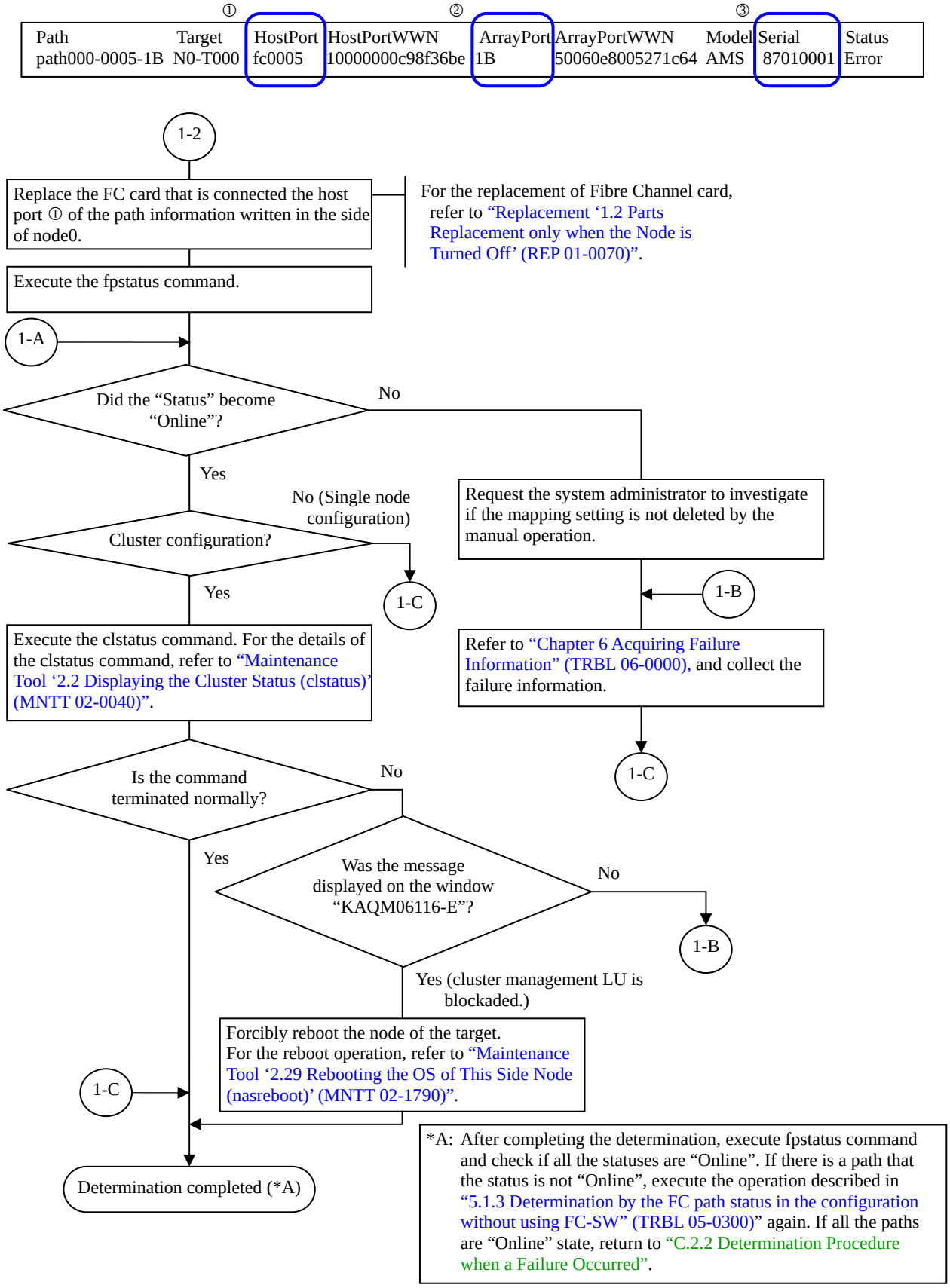


Figure 5.1.3-1 Procedure 1 for Determining by FC Path Status (3/3)

Copyright © 2010, 2012, Hitachi, Ltd.

(2) Determining failure recovery of case #2 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	③ Model	Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	④ HostPort	HostPortWWN	⑤ ArrayPort	ArrayPortWWN	⑥ Model	Serial	Status
path000-0005-0B	N1-T000	fc0005	10000000c98f26ce	0B	50060e8005271c62	AMS	87010001	Error

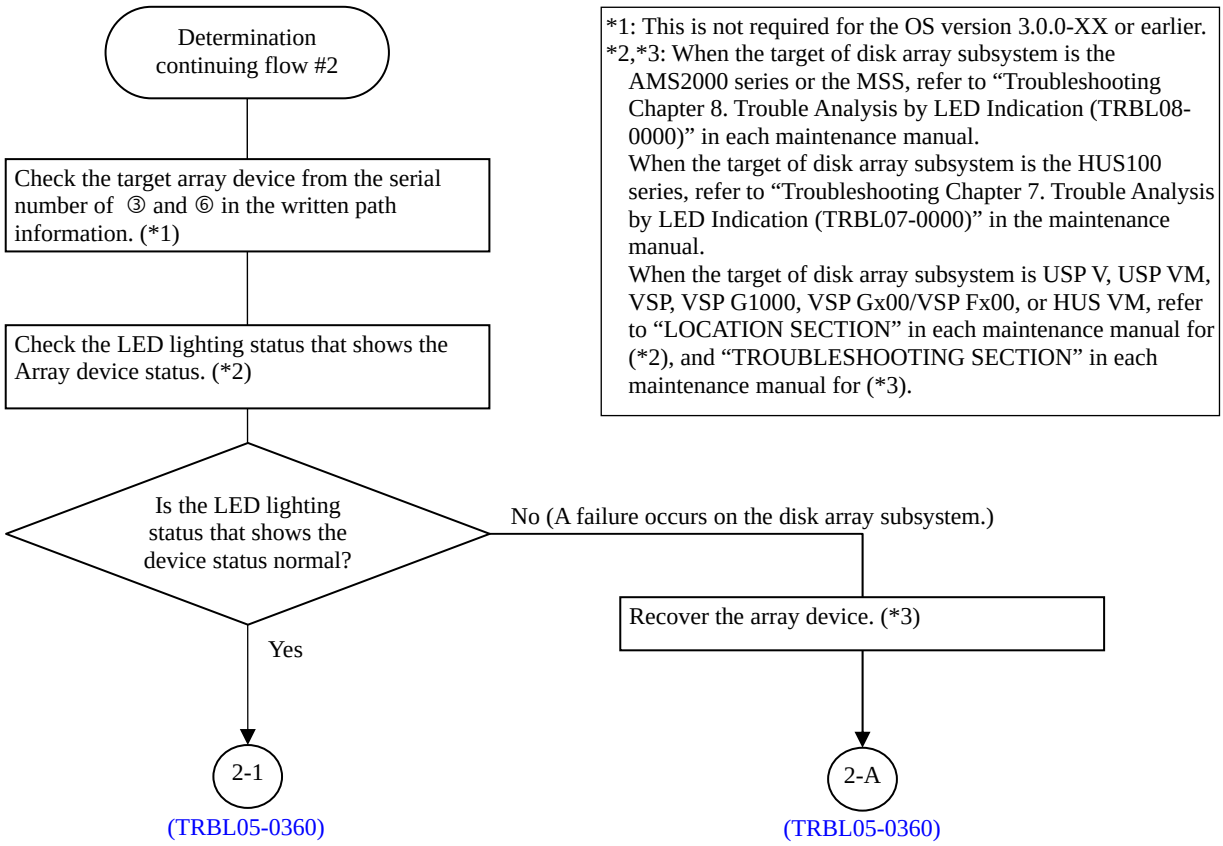


Figure 5.1.3-2 Procedure 2 for Determining by FC Path Status (1/3)

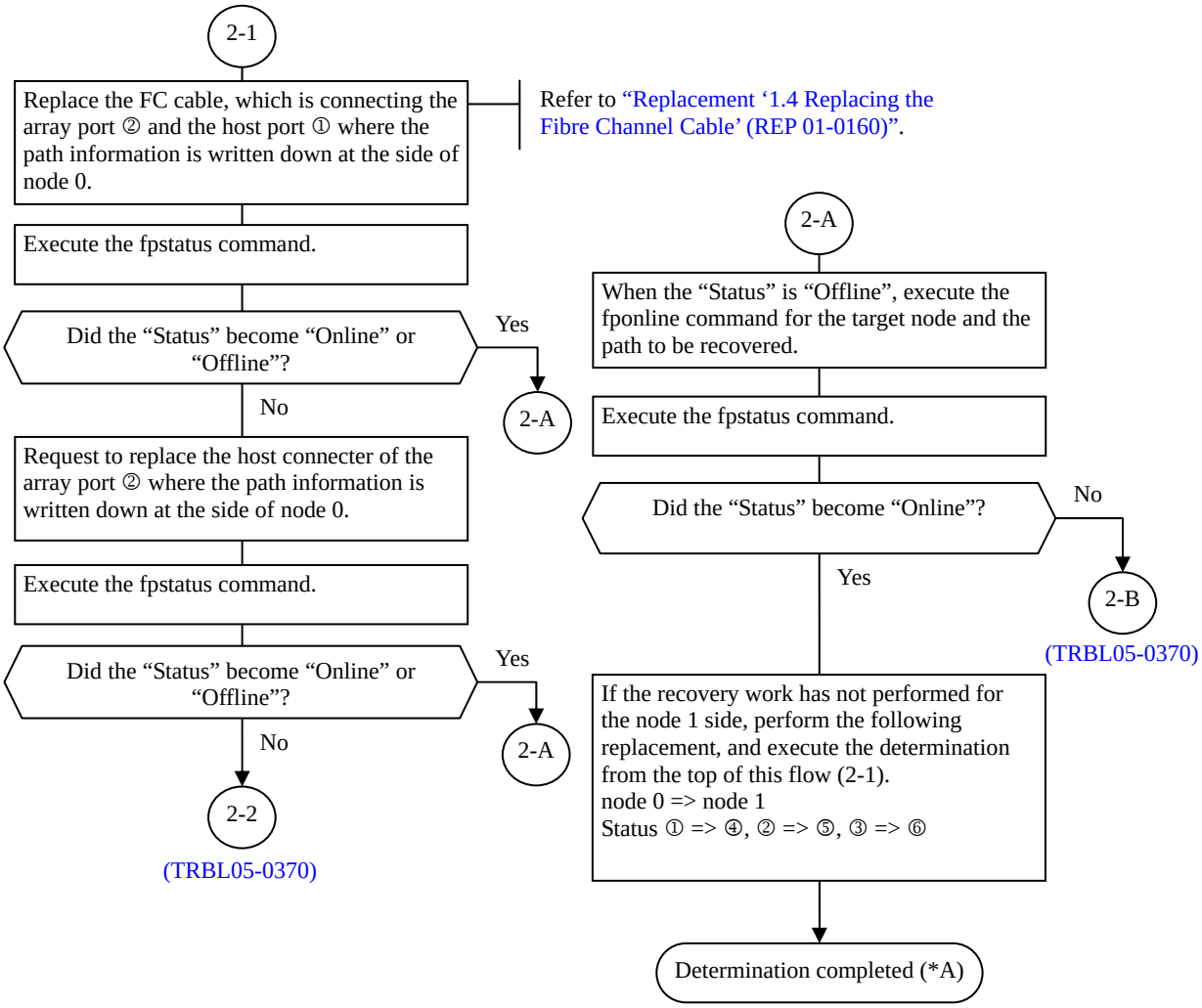
Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	④ HostPort	HostPortWWN	⑤ ArrayPort	ArrayPortWWN	Model	⑥ Serial	Status
path000-0005-0B	N1-T000	fc0005	10000000c98f26ce	0B	50060e8005271c62	AMS	87010001	Error



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online".
If there is a path that the status is not "Online," execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300)" again.
If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-2 Procedure 2 for Determining by FC Path Status (2/3)

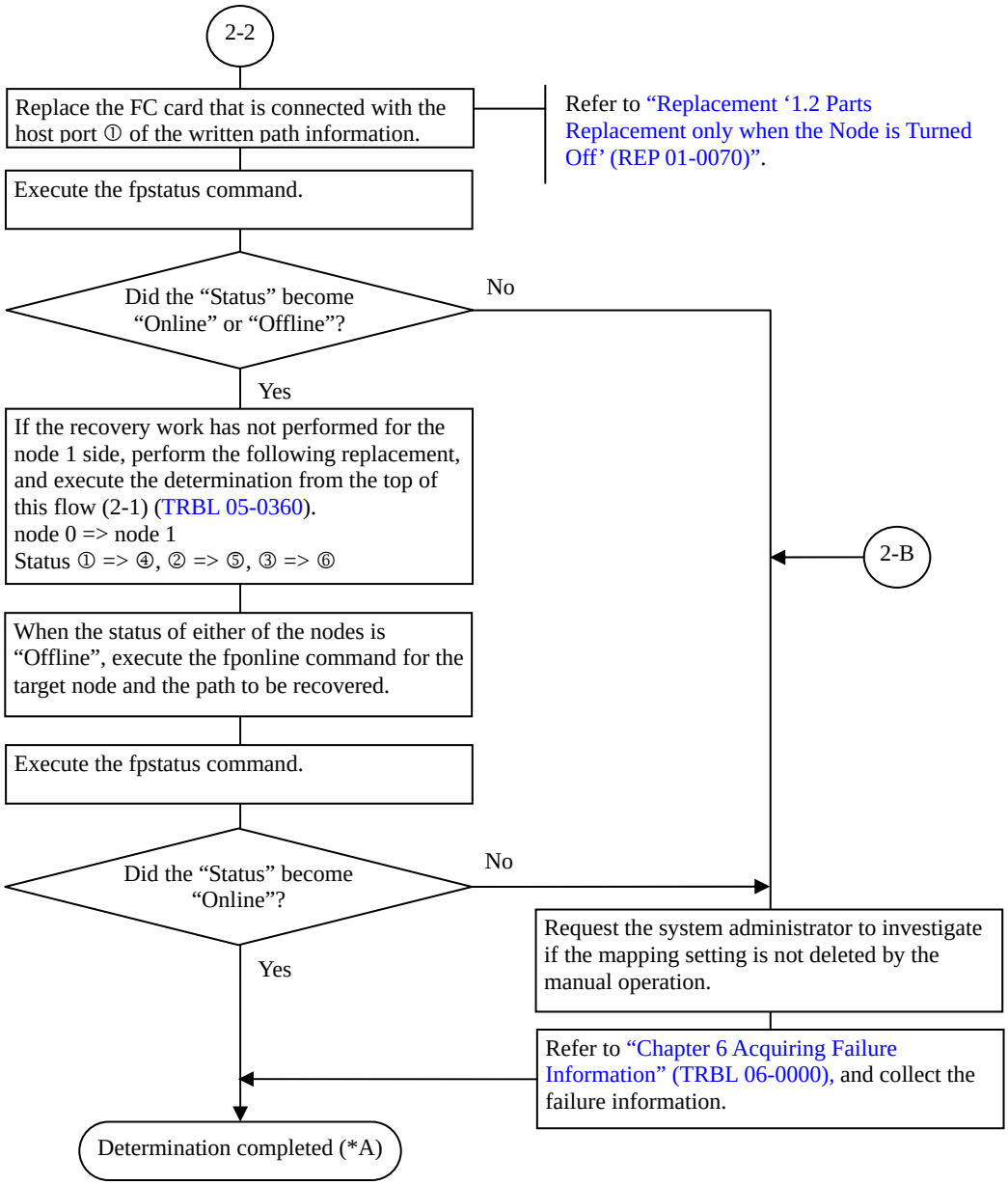
Copyright © 2010, 2014, Hitachi, Ltd.

node0

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	③ Serial	Status
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	④ HostPort	HostPortWWN	⑤ ArrayPort	ArrayPortWWN	Model	⑥ Serial	Status
path000-0005-0B	N1-T000	fc0005	10000000c98f26ce	0B	50060e8005271c62	AMS	87010001	Error



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300)" again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-2 Procedure 2 for Determining by FC Path Status (3/3)

Copyright © 2010, 2014, Hitachi, Ltd.

(3) Determining failure recovery of case #3 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN	ArrayPort ⑤	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

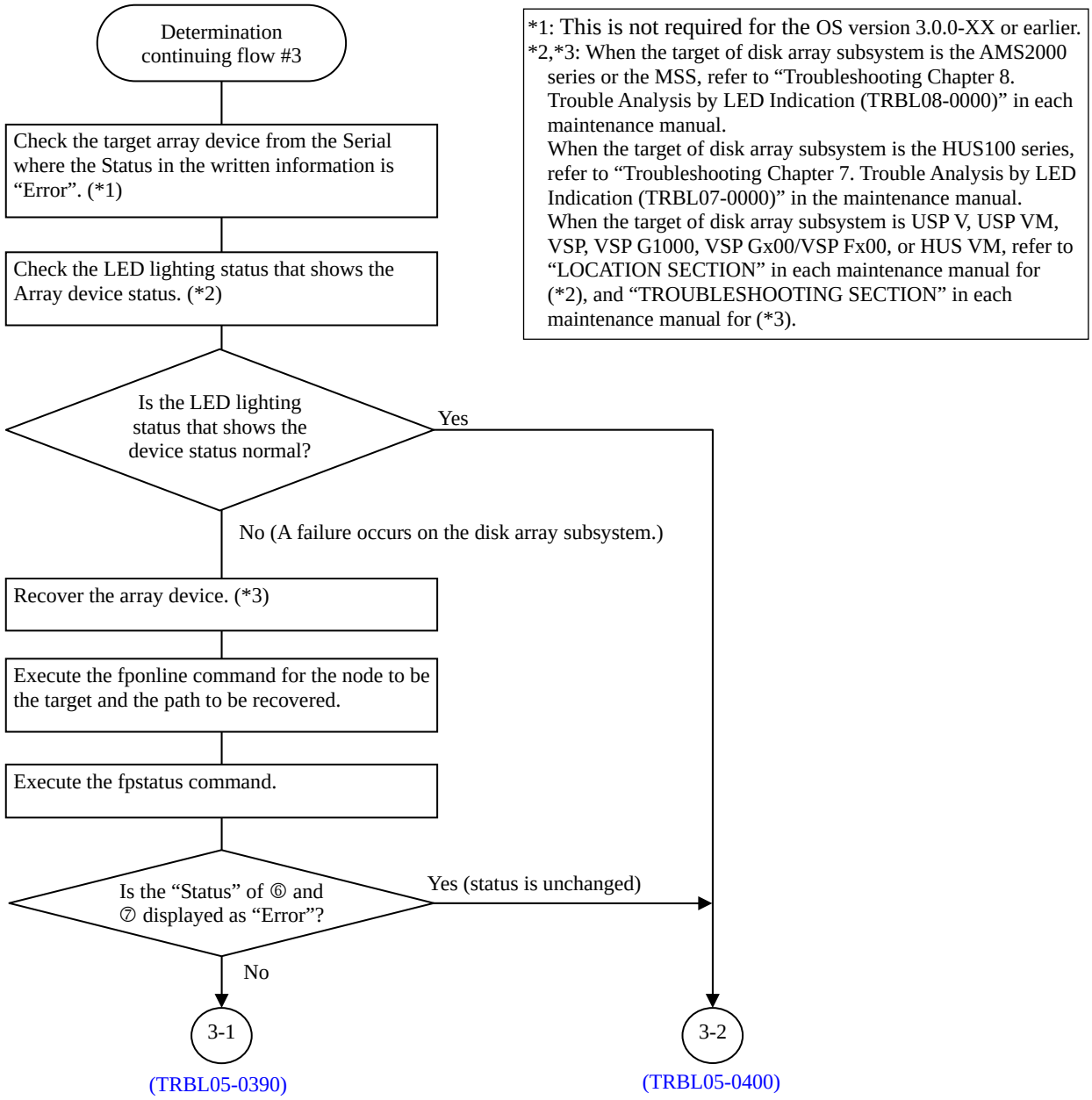


Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (1/6)

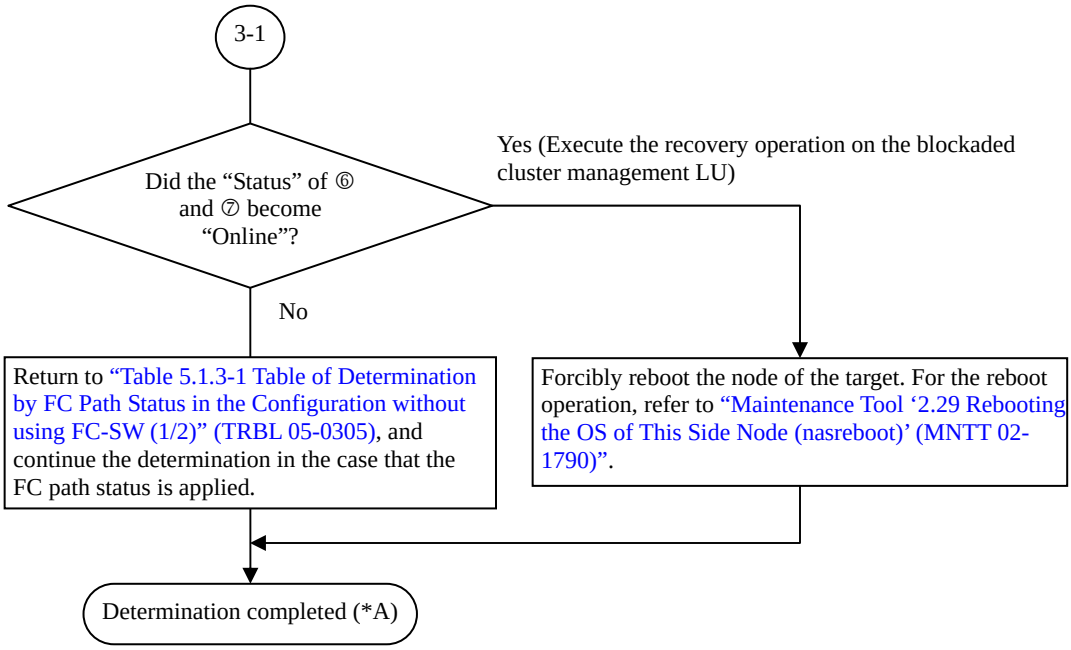
Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN	ArrayPort ②	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN	ArrayPort ⑤	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300)" again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (2/6)

Copyright © 2010, 2012, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

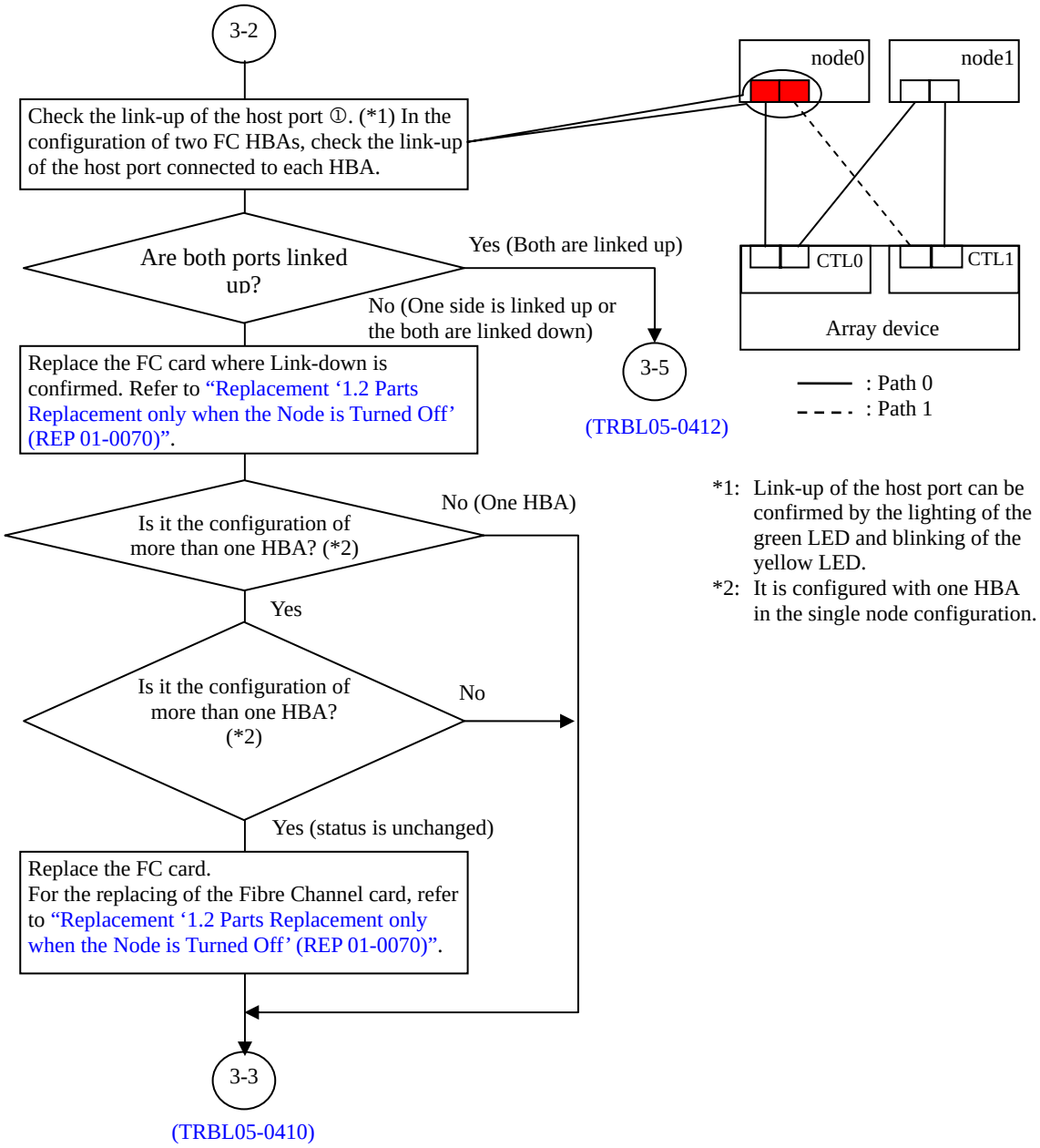


Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (3/6)

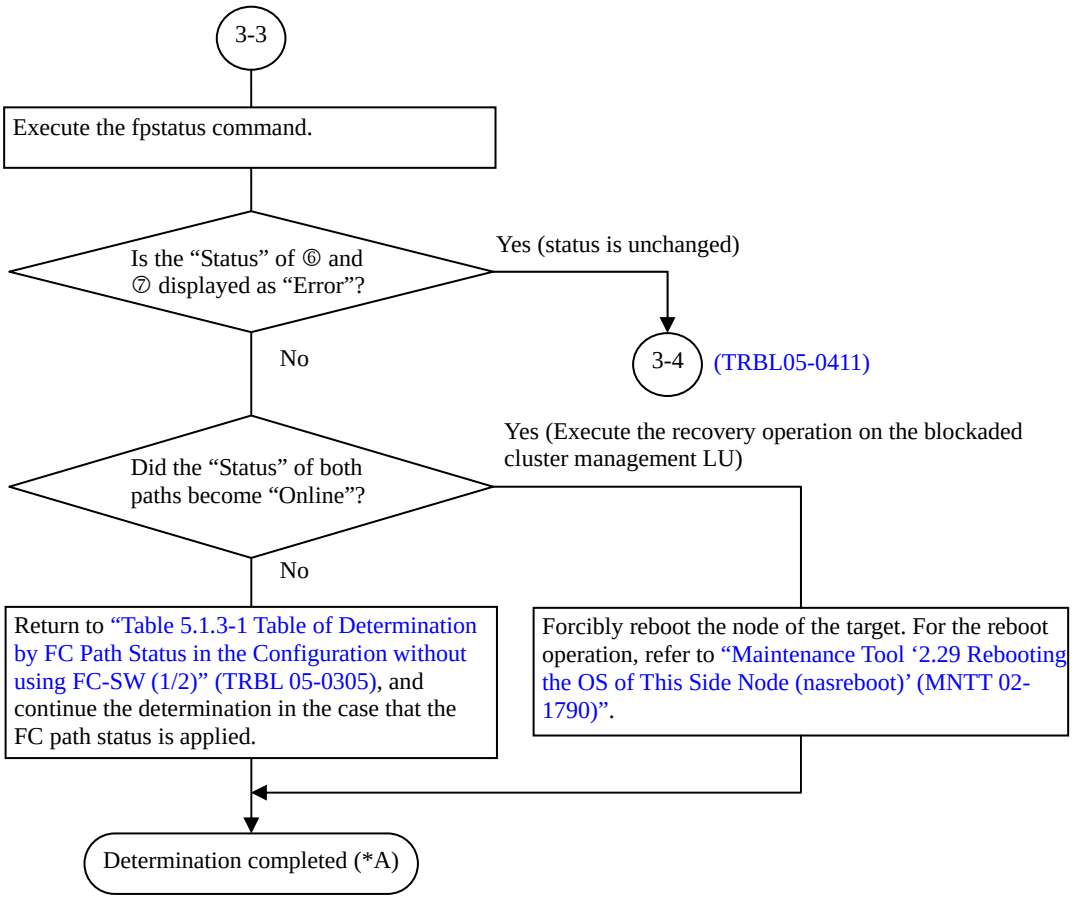
Copyright © 2010, 2014, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial ③	Status	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300) again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (4/6)

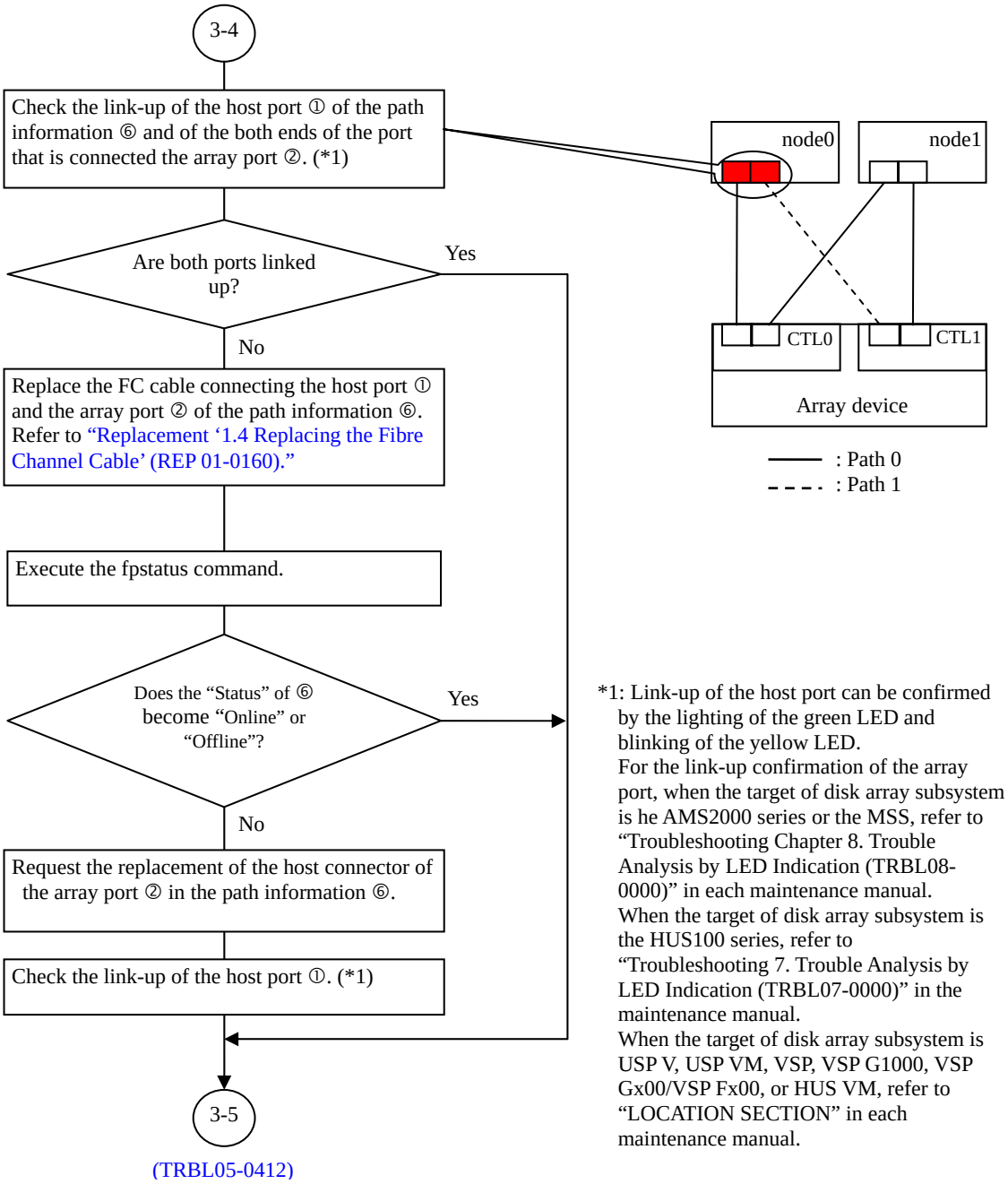
Copyright © 2010, 2012, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial ③	Status	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*1: Link-up of the host port can be confirmed by the lighting of the green LED and blinking of the yellow LED.
For the link-up confirmation of the array port, when the target of disk array subsystem is he AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication (TRBL08-0000)" in each maintenance manual.
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual.

Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (5/6)

Copyright © 2011, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ③	
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error	⑥
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error	⑦

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

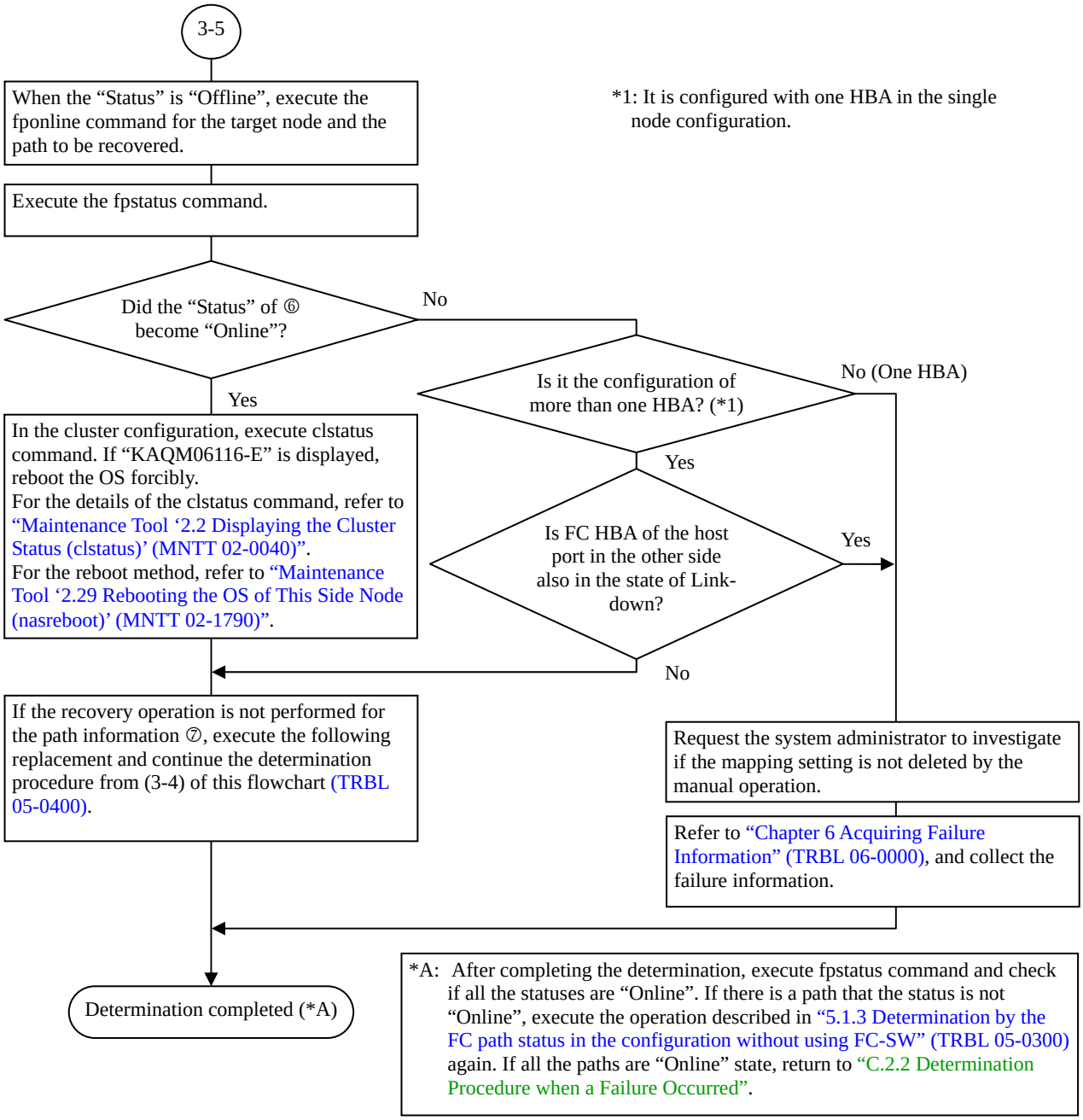


Figure 5.1.3-3 Procedure 3 for Determining by FC Path Status (6/6)

Copyright © 2011, 2012, Hitachi, Ltd.

(4) This page is intentionally blanked.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

(5) Determining failure recovery of case #4 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑤
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	HostPort ③	HostPortWWN ④	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑥
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Error
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Error

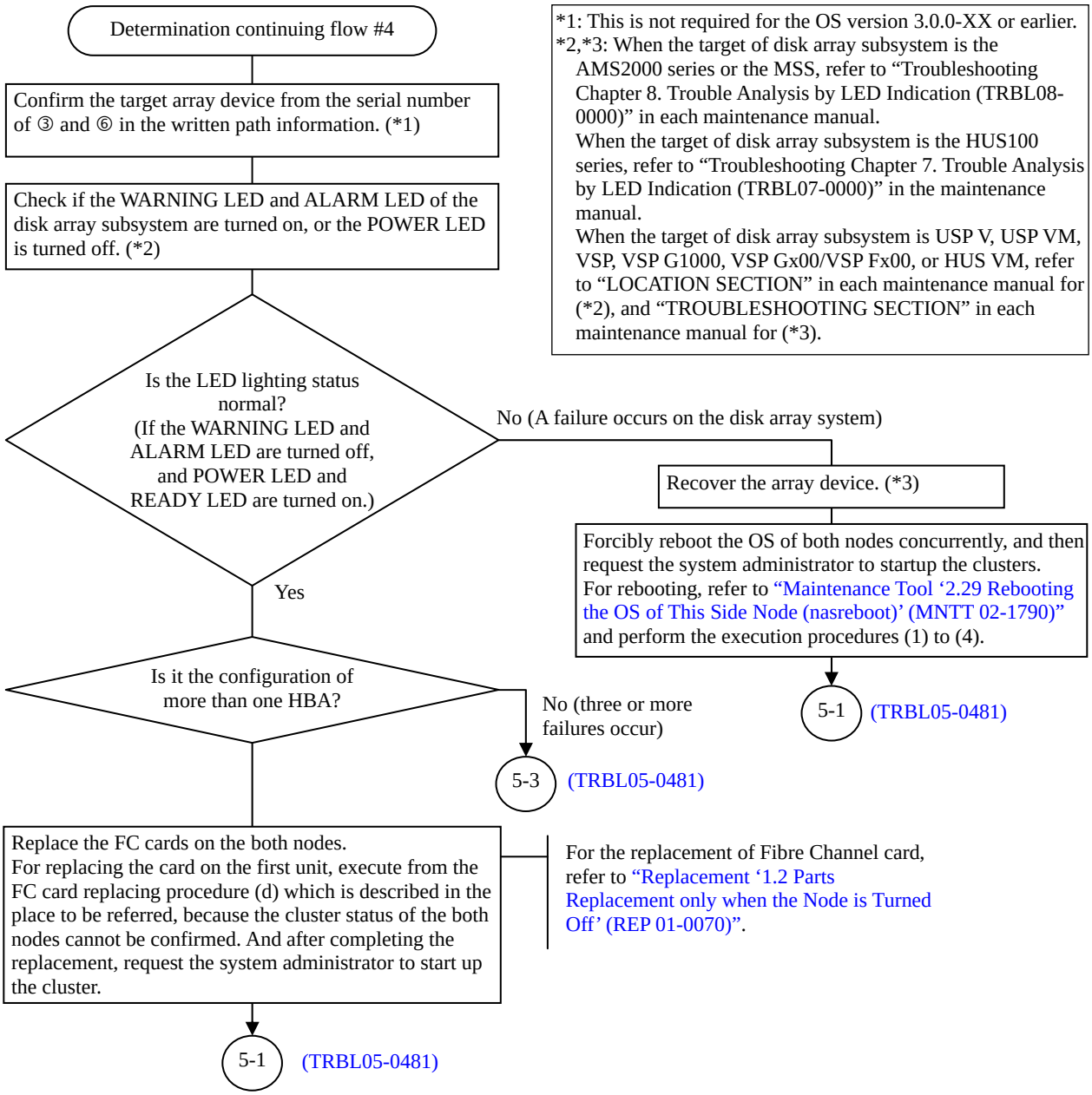


Figure 5.1.3-5 Procedure 5 for Determining by FC Path Status (1/2)

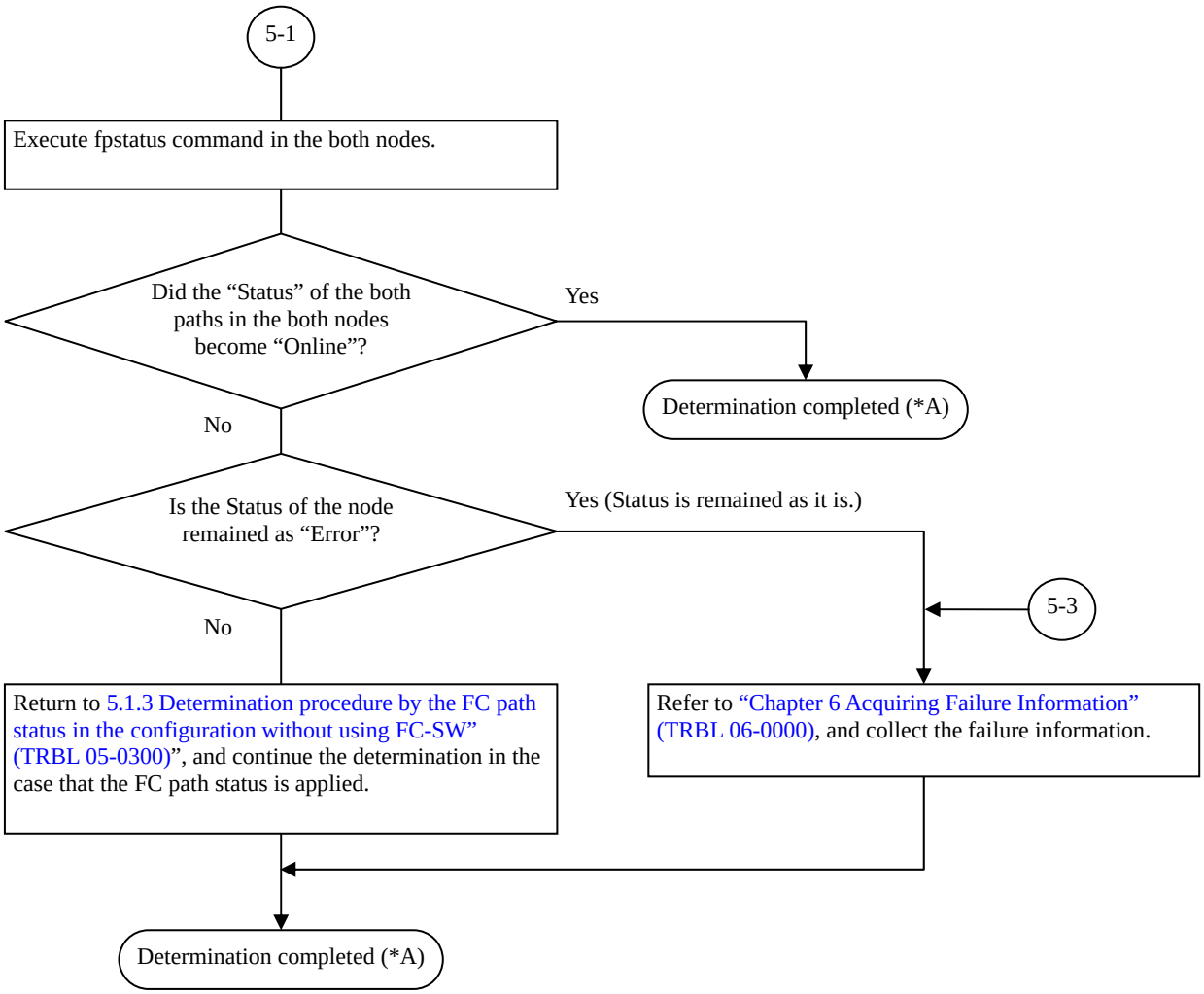
Copyright © 2010, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑤
path000-0004-0A	N0-T000	fc0004	10000000c98f26be	0A	50060e8005271c62	AMS	87010001	Error
path000-0005-1B	N0-T000	fc0005	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Error

node1

Path	Target	HostPort ③	HostPortWWN ④	ArrayPort	ArrayPortWWN	Model	Serial	Status ⑥
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Error
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Error



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300)" again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-5 Procedure 5 for Determining by FC Path Status (2/2)

Copyright © 2011, 2012, Hitachi, Ltd.

(6) Determining failure recovery of case #5 in the table of determination
Based on the written path information, perform the failure analysis in the following procedure, and recover the failure. In this case, there are two type of cases that all the path status become “Unknown” and “Unknown” is shown on one side path and “Configuration Mismatch” is shown on the other side path.

A case when all the path status in the node becomes “Unknown”

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial ③	Status
-	-	fc0004	10000000c98f26be	0A	50060e8005271c62		87010001	Unknown
-	-	fc0005	10000000c98f36be	1B	50060e8005271c64		87010001	Unknown

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online

A case when “Unknown” and “Configuration Mismatch” are mixed in the path status in the node

node0

Path	Target	HostPort ①	HostPortWWN ②	ArrayPort	ArrayPortWWN	Model	Serial ③	Status
-	-	fc0004	10000000c98f26be	0A	50060e8005271c62	-	87010001	Unknown
path000-0006-1B	N0-T000	fc0006	10000000c98f36be	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch
-	-	fc0005	10000000c98f66ab	0A	50060e8005271c64	-	87010001	Unknown
path001-0007-1B	N0-T001	fc0007	10000000c98f76cd	1B	50060e8005271c64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort ④	HostPortWWN ⑤	ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0006-0B	N1-T000	fc0006	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online
path001-0005-1A	N1-T001	fc0005	10000000c98e77ca	1A	50060e8005266b86	AMS	87010012	Online
path001-0007-0B	N1-T001	fc0007	10000000c98e63eb	0B	50060e8005266b88	AMS	87010012	Online

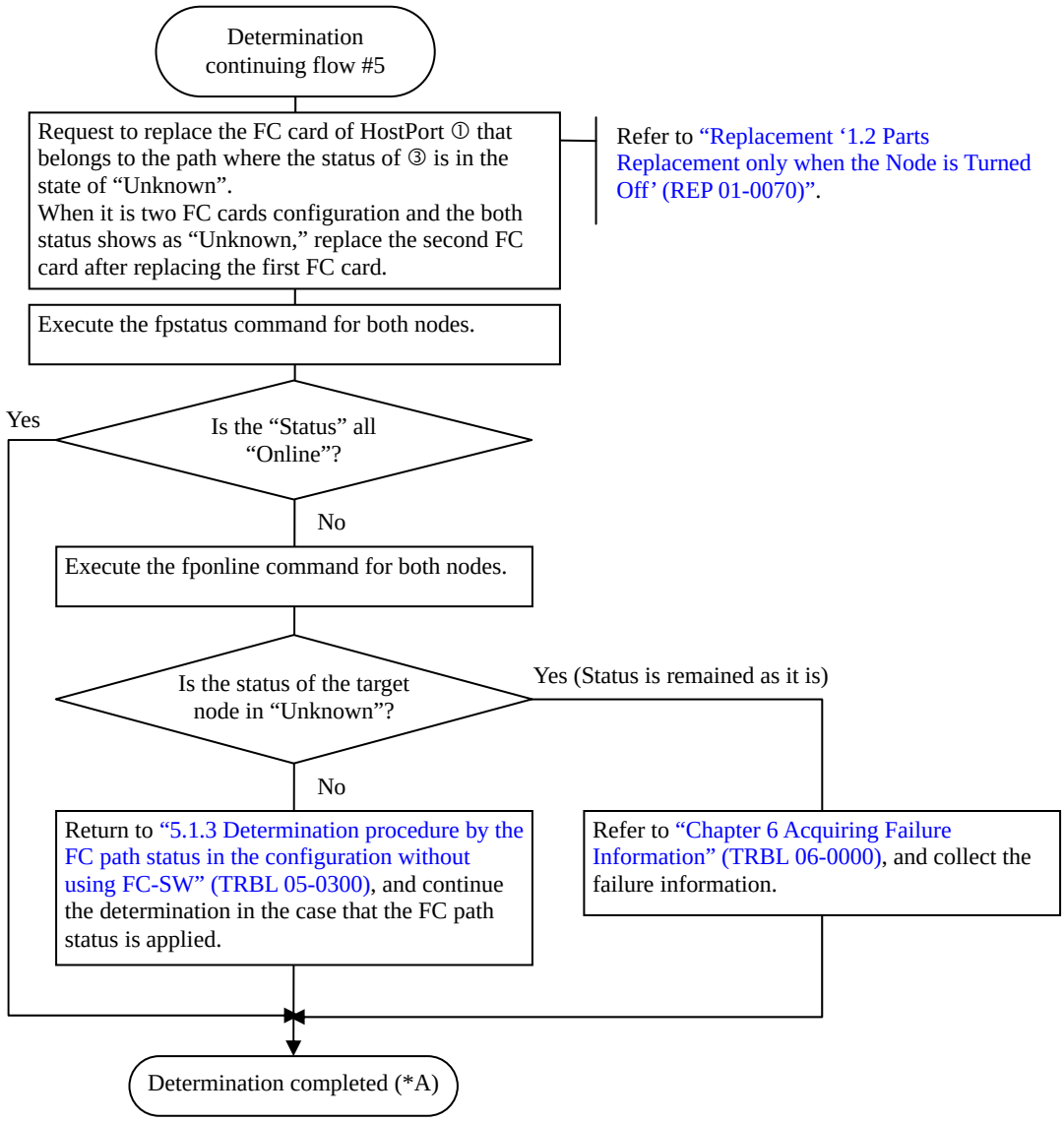
Copyright © 2010, 2011, Hitachi, Ltd.

node0

Path	Target	① HostPort	HostPortWWN	② ArrayPort	ArrayPortWWN	Model	Serial	③ Status
-	-	fc0004	10000000c98f26be	0A	50060e8005271c62		87010001	Unknown
-	-	fc0005	10000000c98f36be	1B	50060e8005271c64		87010001	Unknown

node1

Path	Target	④ HostPort	HostPortWWN	⑤ ArrayPort	ArrayPortWWN	Model	Serial	Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ab	1A	50060e8005271c60	AMS	87010001	Online
path000-0005-0B	N1-T000	fc0005	10000000c98f37bc	0B	50060e8005271c68	AMS	87010001	Online



*A: After completing the determination, execute fpstatus command and check if all the statuses are "Online". If there is a path that the status is not "Online", execute the operation described in "5.1.3 Determination by the FC path status in the configuration without using FC-SW" (TRBL 05-0300) again. If all the paths are "Online" state, return to "C.2.2 Determination Procedure when a Failure Occurred".

Figure 5.1.3-6 Procedure 6 for Determining by FC Path Status

Copyright © 2011, 2012, Hitachi, Ltd.

(7) Determining failure recovery of case #6 in the table of determination
When the FC path status includes “Configuration Mismatch”, operation errors (setting errors at the time of adding the mapping, fpstatus command is executed after rebooting OS) are considered. Therefore, perform the following.

Refer to (a) when the OS version is 2.2.1-XX or earlier, and refer to (b) when the OS version is 3.0.0-XX or later. For the confirmation of the OS version, refer to “Maintenance Tool ‘2.34 Displaying the Version of the OS (versionlist)’ (MNTT 02-2060)”.

(a) When the OS version is 2.2.1-XX or earlier

- When the FC path status is "Configuration Mismatch" for both in the path0 and path1 as below:

```
$ sudo fpstatus
Path              Target     HostPort HostPortWWN       ArrayPort  ArrayPortWWN      Status
path000-0004-0A N0-T000  fc0004   10000000c98f26be  0A          50060e800044b632  Configuration Mismatch
path000-0005-1B N0-T000  fc0005   10000000c98f36be  1B          50060e800044b634  Configuration Mismatch
```

FC path status after fpstatus command execution	Action to be taken
path0 : Configuration Mismatch path1 : Configuration Mismatch	Request the system administrator to check if there is no error in operation (such as setting errors at the time of adding the mapping).

- When the FC path status is " Configuration Mismatch " either in the path0 or in the path1, and nothing is displayed in the other one as below:

```
$  sudo fpstatus
Path              Target     HostPort  HostPortWWN       ArrayPort  ArrayPortWWN      Status
path000-0004-0A  N0-T000  fc0004    10000000c98f26be  0A          50060e800044b632  Configuration Mismatch
```

FC path status after fpstatus command execution	Action to be taken	
path0 : Configuration Mismatch path1 : No display	→ path0 : Online path1 : Error	Regarded as path 0= “Online” and path1 = “Error” as the description in the left, and determine with the “Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)” (TRBL 05-0305).

Copyright © 2010, 2012, Hitachi, Ltd.

(b) When the OS version is 3.0.0-XX or later

(b-1) When the path0 and the path1 of the FC path status are “Configuration Mismatch” and the value of “Serial” and “Target” are the same as shown in the following.

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path000-0005-1B   N0-T000  fc0005    10000000c98f36be  1B        50060e800044b634  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (the values in Serial and Target are the same)	Execute "fpstatus--lipath" command, and check if there is a LU that does not have a replacing path. If there is such LU, request the system administrator to map the subject of LU. If there is no such LU, request the system administrator to confirm if there is any miss operation (setting failure on mapping and so on). For the details of fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

(b-2) When the path0 and the path1 of the FC path status are “Configuration Mismatch” and the value of “Serial” is the same but the value of “Target” is different (Four paths are displayed normally but only two paths are displayed by the failure.)

```
$ sudo fpstatus - v
Path              Target   HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000  fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path001-0005-1B   N0-T001  fc0005    10000000c98f36be  1B        50060e800044b634  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (The value of Serial is the same but the value of Target is different.)	Troubleshooting “Figure 5.1.3-7 Procedure 7 for Determining by FC Path Status” (TRBL05-0503)

Copyright © 2011, 2012, Hitachi, Ltd.

(b-3) The path0 and the path1 of the FC path status are “Configuration Mismatch,” but the value of “Serial” and “Target” are different (in the case of multi array configuration)

```
$ sudo fpstatus - v
Path              Target    HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000   fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
path001-0005-0A   N0-T001   fc0005    10000000c98f36be  0A        50060e800044b366  AMS   87010010   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken
Path0 : Configuration Mismatch Path1 : Configuration Mismatch (The value of “Serial” and “Target” are different.)	Execute the corresponding contents described in (b-4) for each Serial and Target.

(b-4) As described in the following, either one of the path0 and the path1 of the FC path status is “Configuration Mismatch,” and the other side FC path status is not displayed. (Two paths are normally displayed, but only one path is displayed as below due to a failure.)

```
$ sudo fpstatus - v
Path              Target    HostPort  HostPortWWN       ArrayPort ArrayPortWWN      Model Serial     Status
path000-0004-0A   N0-T000   fc0004    10000000c98f26be  0A        50060e800044b632  AMS   87010001   Configuration Mismatch
```

FC path status after executing fpstatus command	Action to be taken	
Path0 : Configuration Mismatch Path1 : No display	→ Path0 : Online Path1 : Error	Assume path0 = “Online”, and path1= “Error” as shown in the description in the left, and then determine in reference to “Table 5.1.3-1 Table of Determination by FC Path Status in the Configuration without using FC-SW (1/2)” (TRBL 05-0305).

Copyright © 2011, Hitachi, Ltd.

node0

Path	Target	HostPort	HostPortWWN	① ArrayPort	ArrayPortWWN	Model	② Serial	③ Status
path000-0006-1C	N0-T000	fc0006	10000000c98f36be	1C	50060e8005271c64	AMS	87010001	Configuration Mismatch
path001-0007-1D	N0-T001	fc0007	10000000c98f56be	1D	50060e8005238b64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort	HostPortWWN	④ ArrayPort	ArrayPortWWN	Model	⑤ Serial	⑥ Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ae	1A	50060e8005271c82	AMS	87010001	Configuration Mismatch
path001-0005-1B	N1-T001	fc0005	10000000c98f47de	1B	50060e8005238b82	AMS	87010001	Configuration Mismatch

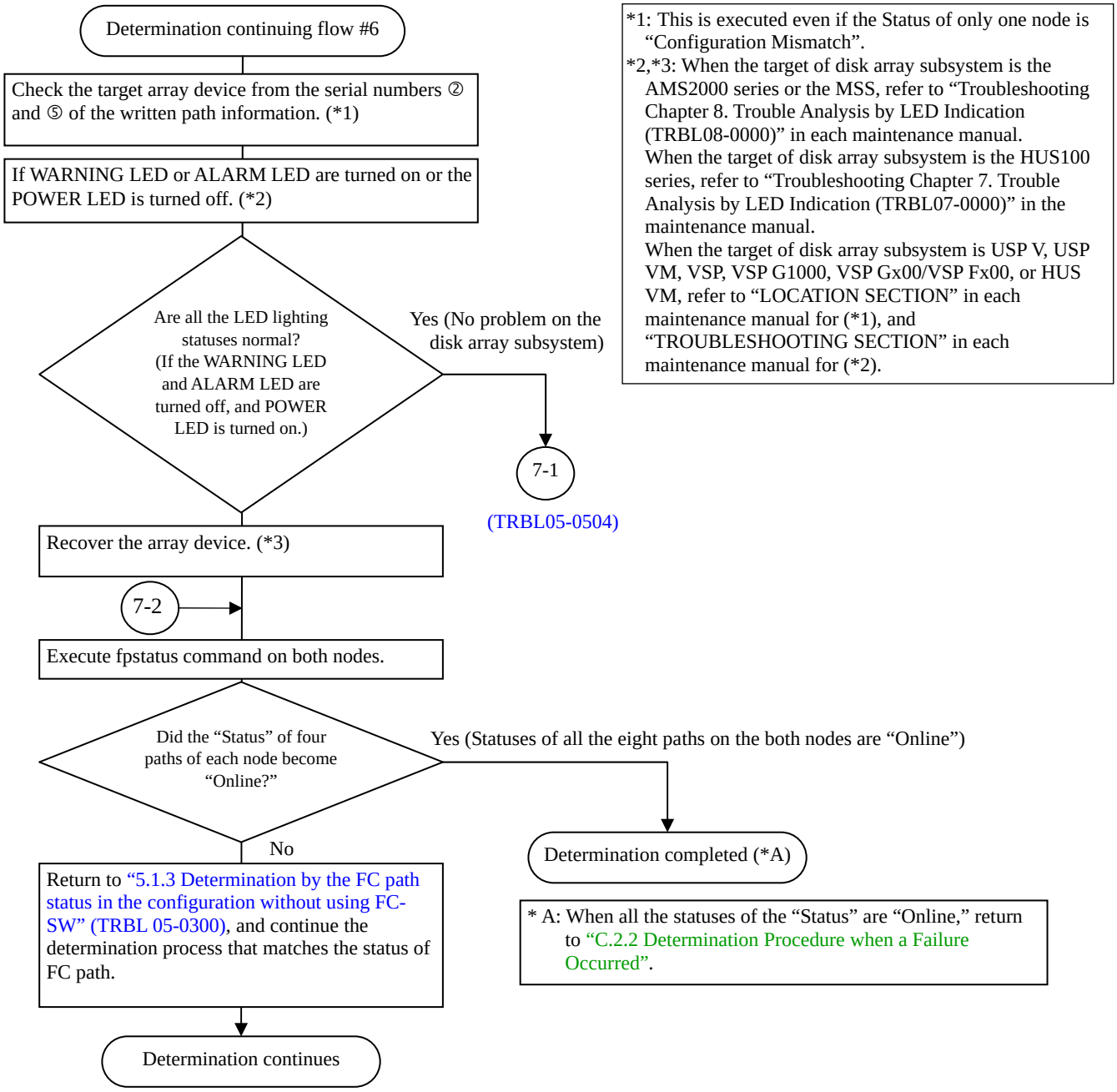


Figure 5.1.3-7 Procedure 7 for Determining by FC Path Status (1/2)

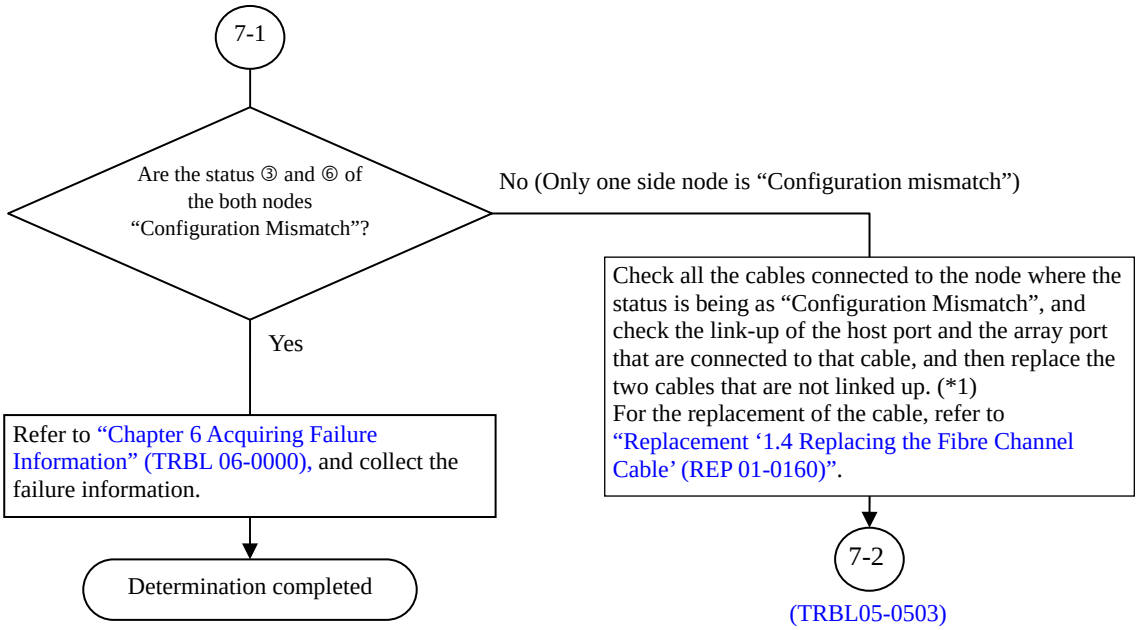
Copyright © 2011, 2016, Hitachi, Ltd.

node0

Path	Target	HostPort	HostPortWWN	① ArrayPort	ArrayPortWWN	Model	② Serial	③ Status
path000-0006-1C	N0-T000	fc0006	10000000c98f36be	1C	50060e8005271c64	AMS	87010001	Configuration Mismatch
path001-0007-1D	N0-T001	fc0007	10000000c98f56be	1D	50060e8005238b64	AMS	87010001	Configuration Mismatch

node1

Path	Target	HostPort	HostPortWWN	④ ArrayPort	ArrayPortWWN	Model	⑤ Serial	⑥ Status
path000-0004-1A	N1-T000	fc0004	10000000c98f27ae	1A	50060e8005271c82	AMS	87010001	Configuration Mismatch
path001-0005-1B	N1-T001	fc0005	10000000c98f47de	1B	50060e8005238b82	AMS	87010001	Configuration Mismatch



*1: Link-up of the host port can be confirmed by the lighting of the green LED and blinking of the yellow LED.
For the link-up of the array port, when the target of disk array subsystem is the AMS2000 series or the MSS, refer to "Troubleshooting Chapter 8. Trouble Analysis by LED Indication' (TRBL08-0000)".
When the target of disk array subsystem is the HUS100 series, refer to "Troubleshooting Chapter 7. Trouble Analysis by LED Indication (TRBL07-0000)" in the maintenance manual.
When the target of disk array subsystem is USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00, or HUS VM, refer to "LOCATION SECTION" in each maintenance manual.

Figure 5.1.3-7 Procedure 7 for Determining by FC Path Status (2/2)

Copyright © 2011, 2016, Hitachi, Ltd.

(8) Determining failure recovery of case #7 in the table of determination
When the FC path status has “Offline” or “Partially Online”, forgetting the procedure after the manual operation is considered. Perform the following.

① Request the system administrator to execute the fponline command for the relevant FC path and change the FC path status to “Online”. Refer to “Maintenance Tool ‘2.9 Switching the FC Path to Online (fponline)’ (MNTT 02-0590)”.
② After completing determination, return to “C.2.2 Determination Procedure when a Failure Occurred”.

(9) Determining failure recovery of case #8 in the table of determination
When it is not applied to any cases in the table of determination, a disk array defect or a dual failure of the device may have occurred or the FC path failure may be recovered.
Execute (9-1) in the case of the cluster configuration and all of the FC path status are “Online”, otherwise execute (9-2.)

(9-1) In the case all of the FC path status are “Online”
① Execute the clstatus command. For the details of the clstatus command, refer to “Maintenance Tool ‘2.2 Displaying the Cluster Status (clstatus)’ (MNTT 02-0040)”.

② Execute ③ if the error message “KAQM06116-E” was displayed as the execution result, otherwise execute (9-2).

③ Reboot the OS of both nodes forcibly because the cluster management LU is blocked. For the reboot operation, refer to “Maintenance Tool ‘2.29 Rebooting the OS of This Side Node (nasreboot)’ (MNTT 02-1790)” and perform the execution procedures (1) to (4).

④ After completing the operation above, return to “C.2.2 Determination Procedure when a Failure Occurred”.

(9-2) In the case of other than (9-1)
① Refer to Troubleshooting “Chapter 6 Acquiring Failure Information” (TRBL 06-0000), and collect the failure information.

② After collecting the information, contact the support center and follow the instructions.

③ After completing determination, return to “C.2.2 Determination Procedure when a Failure Occurred”.

Copyright © 2010, 2014, Hitachi, Ltd.

5.2 Determining Hardware Failures or Software Failures

The failure determination of the hardware failure or the software failure led by the failure determination flow of "C.2.2.2 Failure determination procedure in the single node configuration" is described.

In the cluster configuration, the determination flow of the node failure differs depending on either failover has not occurred or failover occurred and a SIM of failover was displayed or not. Next, determining the node failure when failover has not occurred and when failover occurred are described.

For the determination of the node failure when failover has not occurred, refer to "C.2.3.3 Determining the node failure when failover has not occurred".
For the determination of the node failure when failover occurred, refer to "C.2.3.4 Determining the node failure when failover occurred".

In the single node configuration, refer to "C.2.3.5 Determination of node failure in the single node configuration".

Copyright © 2010, 2012, Hitachi, Ltd.

5.3 Measures when Releasing the LU Access Protection Failed

The description below is the action to be taken when the SIM of releasing LU access protection fails (KAQG72030-E) is displayed.

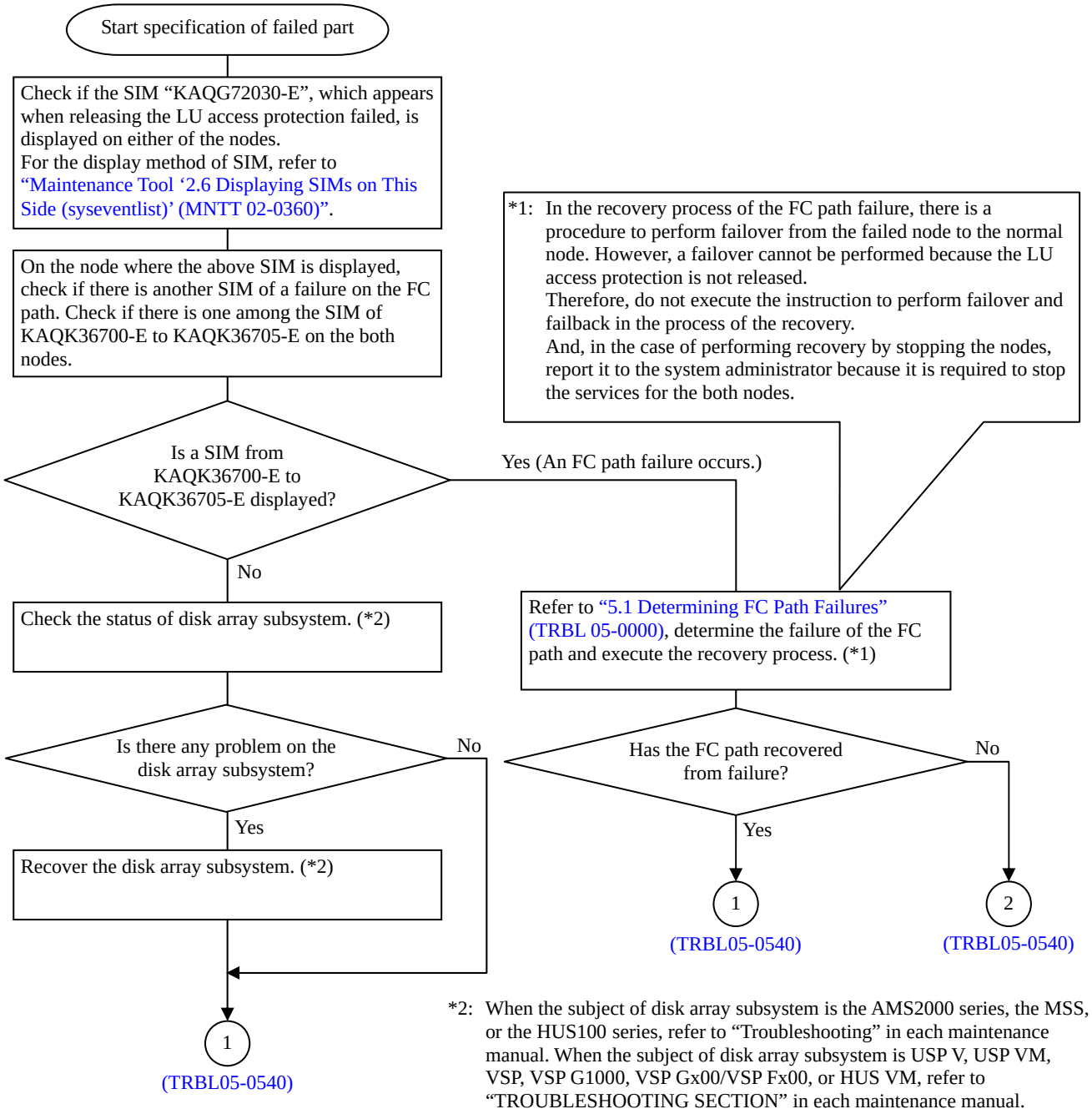


Figure 5.3-1 Determining the failure when releasing the LU Access Protection failed (1/2)

Copyright © 2010, 2016, Hitachi, Ltd.

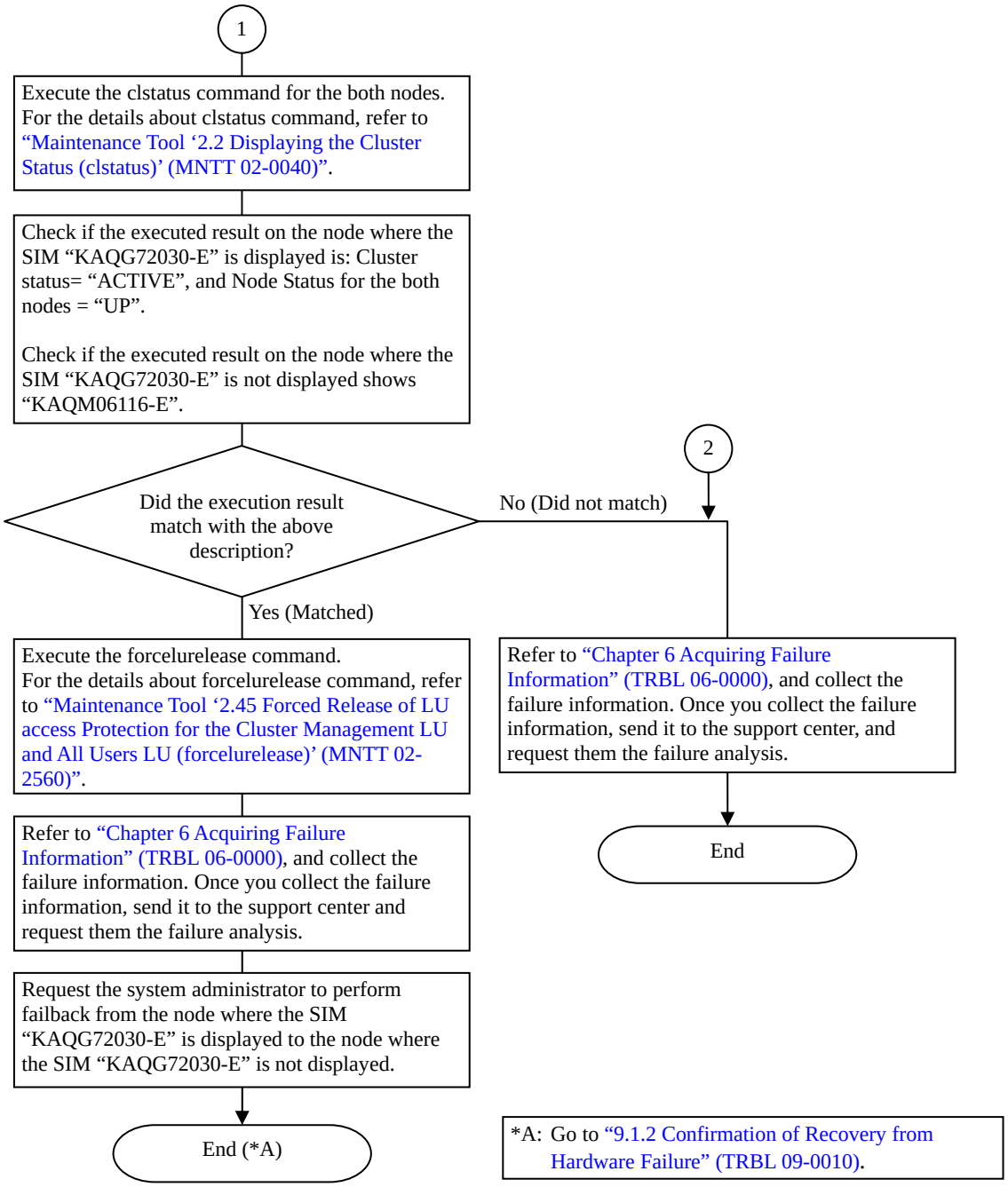


Figure 5.3-1 Determining the failure when releasing the LU Access Protection failed (2/2)

Copyright © 2010, 2014, Hitachi, Ltd.

Chapter 6 Acquiring Failure Information

Acquire the information of the following five failures. However, the disk array failure information is not required in the single node configuration which is not connected to the disk array subsystem.

- Log files
- Dump files
- disk array failure information
- core files
- Internal Log files
- Event Logs (D51B-2U)

Acquiring each piece of failure information is described below.

6.1 Log Files

Log files can be collected during the node operation. However, if the node is not operating due to a failure, the log files cannot be collected. In that case, collect the log files in the maintenance mode.

6.1.1 Acquiring log files

Collect log files by executing the log collection (oslogget) command of the maintenance tool.
Additionally, when the OS version is 4.1.2-XX or earlier, the internal log of the internal RAID controller is also collected.

For collecting log files by the log collection (oslogget) command and in the maintenance mode, refer to "Maintenance Tool '2.19 Collecting Logs (oslogget)' (MNTT 02-1300)".
For collecting the internal log of the internal RAID controller (log.sh), refer to "Maintenance Tool '2.55 Embedded RAID Controller Internal Log Acquisition (log.sh)' (MNTT 02-3080)".

NOTE: For the failure analysis in the cluster configuration, the access information between clusters is required. Collect log files of both nodes in the cluster.
Furthermore, send the collected log files to the Technical Support Center.

Copyright © 2010, 2015, Hitachi, Ltd.

6.1.2 Supplement

The file capacity, the acquisition content of log files, and the file name to be collected differ by specifying log file types (normal, detail or full). Table 6.1.2 shows the acquisition content for each log file type. For details, refer to "Maintenance Tool '2.19 Collecting Logs (oslogget)' (MNTT 02-1300)".

Table 6.1.2 Log File Types and Acquisition Contents

#	Log File Type	Acquisition Content
1	normal	Collect log files of the capacity (20MB/node) that can be surely transferred by HiTrack. Furthermore, if the log files are over several generations, collect the most recent one generation. File name : fast_oslog_*(*).tar.gz
2	detail	Collect log files of the maximum capacity (40MB/node) that can be transferred by HiTrack. Furthermore, collect log files of the maximum of 7MB per file, and collect all generations. File name : oslog_*(*).tar.gz
3	full	Collect log files as far as the capacity of the directory for log file acquisition permits. Furthermore, collect log files of the maximum of 13MB per file, and collect all generations. File name : full_oslog_*(*).tar.gz

*: * represents "device serial number_collected date (YYYYMMDDhhmmss)" at Physical node.

Copyright © 2011, Hitachi, Ltd.

6.2 Dump Files

Convert the memory images to files and create dump files triggered by the panic occurrence in Hitachi Data Ingestor, local node reset or remote node reset.

6.2.1 Collecting dump files

For collecting (downloading) dump files, refer to "Maintenance Tool '2.21 Procedure for Collecting Dump Files' (MNTT 02-1400)".

Refer to Troubleshooting "6.2.1.1 Confirmation whether the dump file is downloaded or not" (TRBL 06-0020)", to confirm if the dump file is downloaded.

If dump files are not created, follow the instruction from the Technical Support Center and collect dump files manually. For collecting dump files manually, refer to Troubleshooting "6.2.1.2 Collecting dump files manually (cluster configuration)" (TRBL 06-0030) in the cluster configuration and refer to Troubleshooting "6.2.1.3 Collecting dump files manually (single node configuration)" (TRBL 06-0030A) in the single node configuration, and execute the collection.

When the node is in the state of not working due to a failure, log in to the system with the maintenance mode and then download the dump files. When the OS version is 2.2.1-XX or later, if there are unconverted dump files, convert the unconverted dump file and then download it. For more details, refer to "Maintenance Tool '2.21.3 Confirm the existence of unconverted dump file (dumpcheck)' (MNTT 02-1461)".
The confirmation of the OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".

NOTE:
- Obtain dump files of level 4.
  When downloading the dump files of level 4, request the system administrator of the download permission or obtain the dump files of level 4 from the system administrator.
  For the reference place in User's Guide describing the details about downloading dump file by the system administrator, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Downloading a dump file' (GENE 00-0050)" for the cluster configuration or refer to "General 'Reference Place in User's Guide for Operating Procedures Table 5 'Collecting/deleting core files and log files' (GENE 00-0060)" for the single node configuration.
- Due to such as dump output operation failure, the dump files of level 3 and level 4 might be created without level 1 dump file. In that case, request the system administrator to have permission to download the dump files of level 3 and level 4. For details about dump collection, refer to "Maintenance Tool '2.21.1 Collecting dump files' (MNTT 02-1420)".

Copyright © 2010, 2012, Hitachi, Ltd.

6.2.1.1 Confirmation whether the dump file is downloaded or not

Log in to the node via ssh from the maintenance PC, and confirm if the dump files are downloaded in the following directory. For details about logging in from the maintenance PC to a node, and the dump file confirmation procedure, refer to "Maintenance Tool '2.21.1 Collecting dump files' (MNTT 02-1420)".

<Physical node>

- /dump/download/service/dump_YYYYMMDDhhmmss (The directory to be downloaded the level 1 dump file)
- /dump/download/all/dump_YYYYMMDDhhmmss (The directory to be downloaded the level 4 dump files)

"YYYYMMDDhhmmss" represents Year, Month, Date, Hour, Minute, and Second.

When the dump file is confirmed that there are existed in that directory, compare the dates between the dump file on the maintenance PC and the dump files on the OS if they are the same or not to confirm if they are already downloaded or not. If it is not downloaded, refer to "Maintenance Tool '2.21.1 Collecting dump files' (MNTT 02-1420)", and collect the dump files.

Figure 6.2.1.1-1 and Figure 6.2.1.1-2 at the Physical node show examples of the directories to be downloaded the dump files of level 1 and 4, and the confirmation of downloading the dump files.

```
$ ls -lL /dump/download/service/dump_20100312135128
total 277248
-r-------- 1 service service  37169408 2010-03-12 13:52 dump_9PSLNBX_20100312135128.lv1.cz.aa
-r-------- 1 service service 246728704 2010-03-12 13:52 dump_9PSLNBX_20100312135128.lv1.cz.ab
```

Figure 6.2.1.1-1 Dump file confirmation (Level 1 at Physical node)

```
$ ls -lL /dump/download/all/dump_20100312135128
total 782636
-r-------- 1 service service  37169408 2010-03-12 13:52 dump_9PSLNBX_20100312135128.lv1.cz.aa
-r-------- 1 service service 246728704 2010-03-12 13:52 dump_9PSLNBX_20100312135128.lv1.cz.ab
-r-------- 1 service service      2438 2010-03-12 13:59 dump_9PSLNBX_20100312135128.lv4.cz.aa
-r-------- 1 service service 273966493 2010-03-12 13:59 dump_9PSLNBX_20100312135128.lv4.cz.ab
```

Figure 6.2.1.1-2 Dump file Confirmation (Level 1 and Level 4 at Physical node)

Copyright © 2010, 2011, Hitachi, Ltd.

6.2.1.2 Collecting dump files manually (cluster configuration)

At the manually collecting dump files in the cluster configuration, the reset request is issued to this side node OS from the other side node. About the reset of the OS, refer to "Maintenance Tool '2.30 Resetting the OS of the Node (nncreset)' (MNTT 02-1840)".

By the resetting process, the node is restarted at the Physical node and dump files are created.

When the OS version is 2.1.1-XX at the Physical node, make sure that the SIM of "KAQK39500-E OS error Detail=05 00 00 00 Level=00 Type=03" that indicates that the success of the dump file creation is displayed after rebooting.

When the OS version is 2.2.1-XX or later, make sure that the SIM of "KAQK39500-E OS error Detail=05 00 00 01 Level=00 Type=03" that indicates the completion of copying the memory image is displayed after rebooting, and after a while, wait until the SIM of "KAQK39528-I Processing to convert dump files ended." that indicates the success of the dump file creation is displayed on the node. (It takes about 30 minutes to create dump files with the amount of 12GB memory installed.)

For the details of confirmation of SIM, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)". If the SIM message is confirmed, download the dump files. For the details of collecting dump files, refer to "Maintenance Tool '2.21.1 Collecting dump files' (MNTT 02-1420)".

For the confirmation of OS version, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)".
After restarting the node, if the SIM of "KAQK39500-E OS error Detail=06 00 03 00 Level=00 Type=03" that indicates a failure of copying the memory image is displayed on the restarted node, dump files for Physical node are not created.

Copyright © 2010, 2012, Hitachi, Ltd.

6.2.1.3 Collecting dump files manually (single node configuration)

The manual dump file collection in the single node configuration is executed by NMI issue operation or issuing a request to reset the OS of this side node. Refer to "Installation '2.1.3.2 OS reboot of a node by NMI issue operation (single node configuration only)' (INST 02-0140)".
For the details of reset request of OS, refer to "Maintenance Tool '2.30 Resetting the OS of the Node (nncreset)' (MNTT 02-1840)". If the OS is running, execute the dump collection with the command of nncreset.
By the resetting process, the node is restarted and dump files are created. Confirm that the SIM of "KAQK39500-E OS error Detail=05 00 00 01 Level=00 Type=03" that indicates the completion of copying the memory image is displayed on the restarted node, and then wait until the SIM of "KAQK39528-I Processing to convert dump files ended." that indicates the success of the dump file creation is displayed on the node. (It takes about 30 minutes to create dump files with the amount of 12GB memory installed.)
For the details of confirmation of SIM, refer to "Maintenance Tool '2.6 Displaying SIMs on This Side (syseventlist)' (MNTT 02-0360)". If the SIM message is confirmed, download the dump files. For the details of collecting dump files, refer to "Maintenance Tool '2.21.1 Collecting dump files' (MNTT 02-1420)".
After restarting the node, if the SIM of "KAQK39500-E OS error Detail=06 00 03 00 Level=00 Type=03" that indicates a failure of copying the memory image is displayed on the restarted node, dump files are not collected.

Copyright © 2011, 2014, Hitachi, Ltd.

6.2.2 Supplement

The downloaded dump files are named as follows at Physical node.

<Dump files at Physical node>

- dump_< device serial number >_<dump collected date>.lv<level>.cz_<segregated identifier>
- dump_< device serial number >_<dump collected date>.lv<level>.cz.<segregated identifier>

  < device serial number >: The device serial number of the collected node
  <dump collected date>: 14-byte character string in YYYYMMDDhhmmss (year/month/day/hour/minute/second) format
  <level>: one-byte character of 1 or 4 (maintenance personnel can collect level 1 only)
  <separated identifier>: Identifier to divide a file. When a dump file exceeds 400MB, changes the identifier, divides dump file and downloads (aa. ab. cc… is attached).

  NOTE: Send the collected log files to the Technical Support Center. Delete the files when all of the dump files are downloaded. For deleting the files, confirm the Technical Support Center. For deleting files, refer to "Maintenance Tool '2.21.2 Deleting dumps (dumpdel)' (MNTT 02-1440)".

Copyright © 2011, 2013, Hitachi, Ltd.

6.3 Disk Array Failure Information

Acquire the following failure information as disk array information.

6.3.1 AMS2000 Series

- Simple trace
- Controller blockade trace
- Full dump

For acquiring disk array failure information, refer to Troubleshooting “Collecting failure information” in the disk array manual “DF800 Disk Array System Maintenance Manual”.

6.3.2 MSS

- Simple trace
- Controller blocked trace
- Full dump

For the acquisition of disk array failure information, refer to Troubleshooting “Collecting failure information” in the disk array manual “DF800E-XS Disk Array System Maintenance Manual”.

6.3.3 HUS100 Series

- Simple trace
- Controller blockade trace
- Full dump

For acquiring disk array failure information, refer to Troubleshooting “Collecting failure information” in the disk array manual “DF850 Disk Array System Maintenance Manual”.

6.3.4 USP V, USP VM, VSP, VSP G1000, VSP Gx00/VSP Fx00 and HUS VM

- Auto Dump

For the acquisition of the controller troubleshooting information, refer to “SVP SECTION” or “MAINTENANCE PC” described in each maintenance manual.

Copyright © 2010, 2016, Hitachi, Ltd.

6.4 Core Files

Acquire core files of Physical node.
For acquiring core files, log in to the node via ssh from the maintenance PC, execute “ls-lL/dump/download/core/”, and confirm if the core file is existed under the (/dump/download/core). For details about logging in from the maintenance PC to a node, refer to “Maintenance Tool ‘1.3.2 Logging in to a node for executing commands’ (MNTT 01-0200)”.

```
$ ls -l /dump/download/core/*
-r-------- 1 service service 335872 2010-03-12 13:58 /dump/download/core/core-10709-sleep-1268369883
```

Figure 6.4-1 Core File Confirmation

The core file name is set as the following.
core-process ID-process name-time of core file (The elapsed second from the Jan.1. 1974).
And confirm the created time of core file from the file attribute (red frame).
After the confirmation of the core file, download it. For downloading files, refer to “Maintenance Tool ‘1.3.5 Commands used for transferring files’ (MNTT 02-0230)”.

NOTE:• core file is deleted automatically after expiring the storage period.

6.5 Internal Log Files

Acquire Internal Log files as HCP information. For acquiring Internal Log files, refer to “Hitachi Content platform Administering HCP”.

For the details of Internal Log file, refer to “Hitachi Content Platform Administering HCP”.

6.6 Event Logs (D51B-2U)

When using D51B-2U, collect Event Log from MegaRAC GUI at the time of the occurrence of the hardware failure. For Format of Event Log, collect the two patterns “Text” and “hex”. For how to log into MegaRAC GUI or how to collect Event Log, refer to “QuantaGrid Series D51B-2U Technical Guide”.

Copyright © 2010, 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2011, Hitachi, Ltd.

Chapter 7 Failure Monitoring by SNMP

In this chapter, the failure monitoring of Hitachi Data Ingestor (HDI) using SNMP is described.

7.1 Failure Notice by SNMP

HDI reports a failure of HDI to the customer's monitoring computer in which the SNMP manager program is installed. By this, the system administrator can detect a failure occurred in HDI. After detecting the failure occurrence, the system administrator reports it to the Technical Support Center (the site where HiTrack is not installed is required to install SNMP).

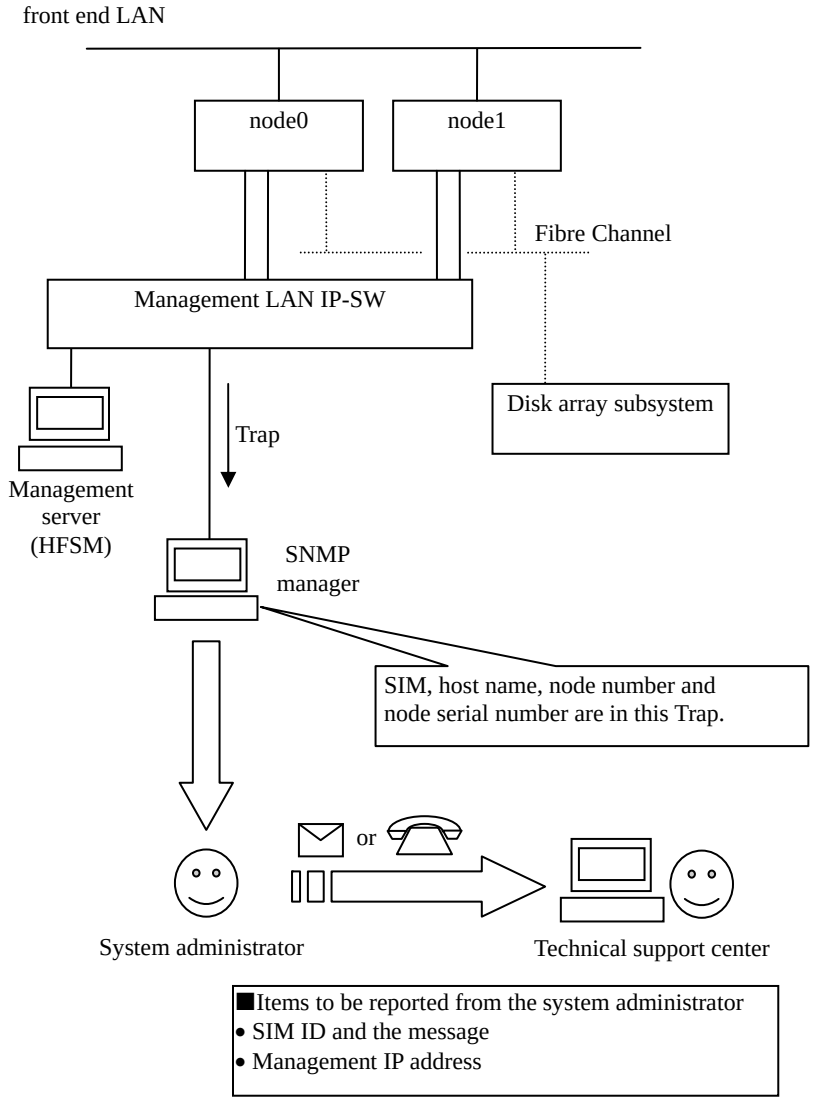


Figure 7.1-1 The flow that a customer notifies the support center of the occurrence of a failure

Copyright © 2010, 2012, Hitachi, Ltd.

7.2 Messages of Trap that the Maintenance Personnel should Obtain

Trap messages are displayed in the following format.

The system administrator checks SIM IDs and the messages from the SNMP Trap. The maintenance personnel obtains SNMP Trap that is reporting the message ID of SIM from the system administrator. Table 7.2-1 shows the list of Trap messages to be obtained by the maintenance personnel.

■ Display examples of SNMP Trap

KAQG46040-E An error message is sent to maintenance personnel.
(SIM ID: KAQG39504-E Link down in Front-end LAN.)

Trap message ID
(not a SIM ID)

SIM ID and message
stored in the Trap

Table 7.2-1 SNMP Trap to be sent by HDI

#	Trap message ID	Trap Message	SIM ID stored in the Trap (*)
1	KAQG46040-E	An error message is sent to maintenance personnel. (SIM ID: KAQxnnnnn-E <*message*>)	KAQxnnnnn-E
2	KAQG46041-W	A warning message is sent to maintenance personnel. (SIM ID: KAQxnnnnn-W <*message*>)	KAQxnnnnn-W
3	KAQG46042-I	An information message is sent to maintenance personnel. (SIM ID: KAQxnnnnn-I <*message*>)	KAQxnnnnn-I

Legend: x: alphabetical character
n: numeric character

*: Trap message IDs differ depending on the level of SIM.
E (failure level) reports KAQG46040-E, W (warning message) reports KAQG46041-W, and I (progress message) reports KAQG46042-I.

NOTE: When the failure monitoring is executed with the SNMP manager without introducing HiTrack, you must perform* polling from the SNMP manager to the maintenance port of each node at the cluster configuration, or to the port used in the operation at the single node configuration, with SNMP GET.
If you fail the polling with SNMP GET due to the communication failure, you need to call the maintenance personnel for the maintenance.

*: The setting must be that a warning is displayed if the value cannot be obtained by executing the polling of SNMP GET for the standard MIB 1.3.6.1.2.1.4.20.1.1 (IPv4 address). When IPv6 address is set, the value cannot be obtained with the standard MIB. Therefore, use the Hitachi extension:
MIB 1.3.6.1.4.1.116.5.11.5.1.1.6.1.1.4 (IP address (IPv6 address)).

Copyright © 2010, 2012, Hitachi, Ltd.

7.3 Failure Notice by E-Mail

HDI reports a failure of HDI to the mail address which the system administrator specified.
After detecting the failure occurrence, the system administrator reports it to the Technical Support Center.

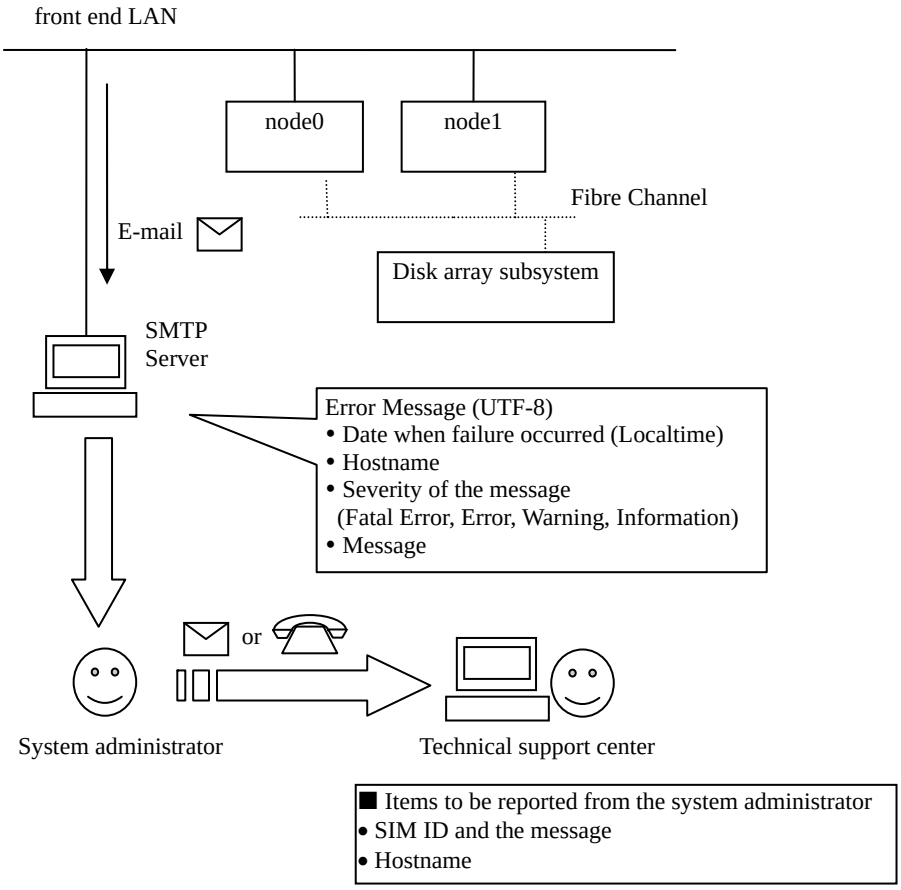


Figure 7.3-1 The flow that a customer notifies the support center of the occurrence of a failure

Copyright © 2012, Hitachi, Ltd.

7.4 Messages of E-mail that the Maintenance Personnel should Obtain

The system administrator checks message IDs and the messages from the E-mail. The maintenance personnel obtains E-mail that is reporting the message ID from the system administrator.

The following example show example of the failure notice which is sent by E-mail

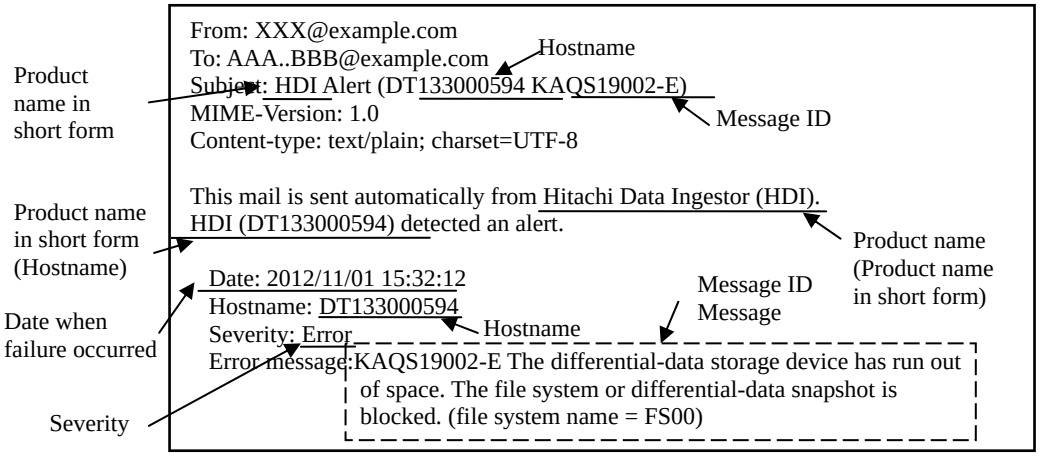


Figure 7.4-1 Display examples of failure notice by E-mail

Copyright © 2012, Hitachi, Ltd.

Chapter 8 Messages

For the messages, refer to “C.3 Messages”.

Copyright © 2010, 2011, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, 2011 Hitachi, Ltd.

Chapter 9 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure

This chapter describes how to confirm the recovery of the entire node after a power supply failure, a management system network failure (cluster configuration only), an FC path failure, or a hardware failure is corrected. This chapter also provides the recovery procedure for a software failure identified through the troubleshooting procedures described in respective chapters of "Troubleshooting" or by a message described in "Chapter 8. Messages".

The determination process is different by the configuration of a cluster or a single node.
For the cluster configuration, refer to "9.1 Confirmation of hardware failure recovery and recovery procedure for software failure at the cluster configuration", and for the single node configuration, refer to Troubleshooting "9.2 Confirmation of hardware failure recovery and recovery procedure for software failure at the single node configuration" (TRBL 09-0640).

9.1 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure at the Cluster Configuration

9.1.1 Overview of Confirmation of the Entire Node after Hardware Failure Recovery and Recovery Procedure for Software Failure

The overview of confirmation of the entire node after recovery from a hardware failure and the overview of software failure recovery are described below.

- Confirmation of the entire node

  When it is necessary to refer to this chapter after hardware replacement or as a result of failure determination flowchart* in "Troubleshooting", refer to Troubleshooting "9.1.2 Confirmation of Recovery from Hardware Failure" (TRBL 09-0010) to check that the entire hardware is in the normal status and there is no other failure.

  *: If the failure is determined as other than a hardware failure, refer to "Software failure recovery" described below.

- Software failure recovery

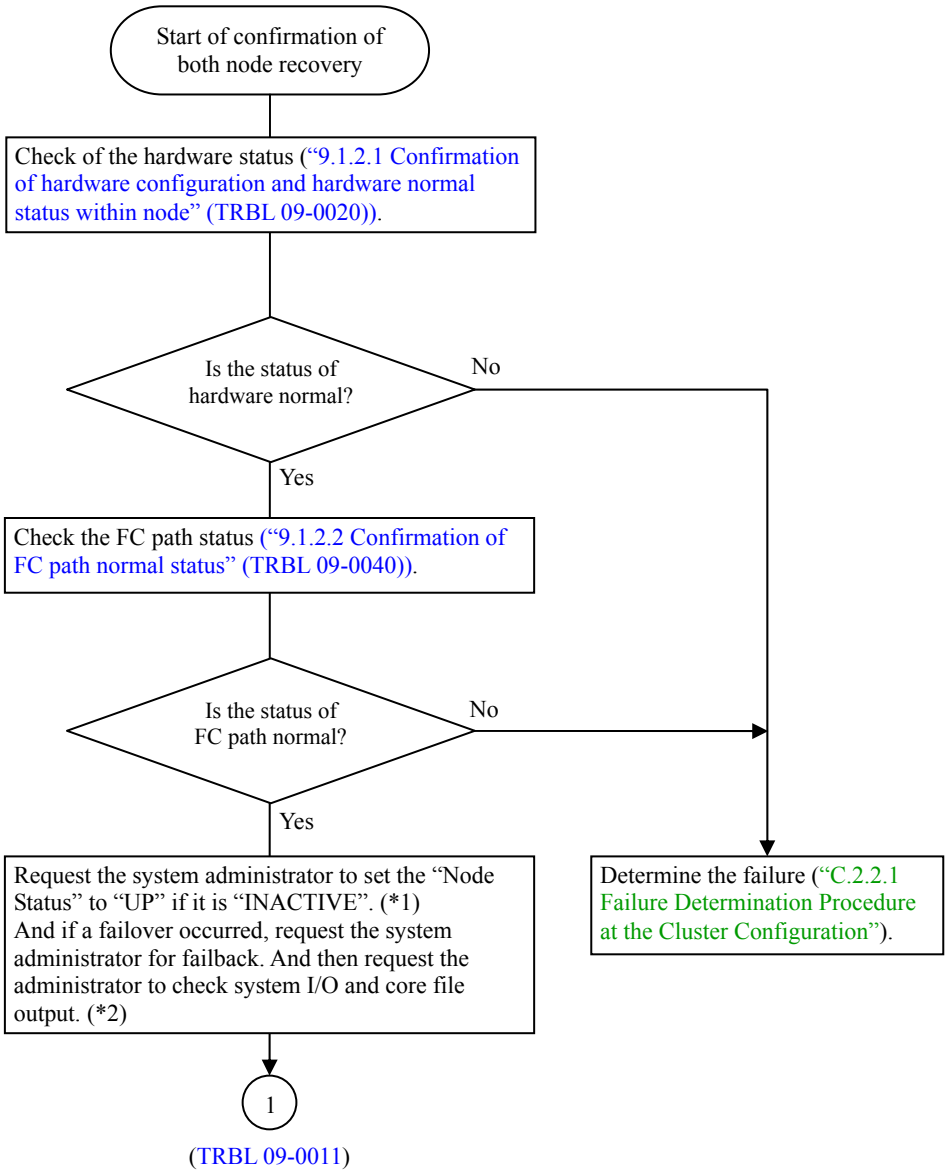
  When it is necessary to refer to this chapter after a SIM message (KAQK3950X-E) concerning a software failure is displayed, refer to Troubleshooting "9.1.3 Recovery Procedure for Software Failure" (TRBL 09-0040) to perform the failure recovery procedure corresponding to the SIM (KAQK3950X-E) and the final recovery procedure.

Copyright © 2014, Hitachi, Ltd.

9.1.2 Confirmation of Recovery from Hardware Failure

Figure 9.1.2-1 show the sequence how to check the recovery completion of hardware failure.

Check if all of the hardware are in normal status, and check if all of the FC path are in normal status.



*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the failback of resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".

*2: A part of Network Interface Card might not be able to perform I/O to the system even if Network Interface Card can link up by Link-up LED or the hwstatus command. In this case, contact the Technical Support Division.

Figure 9.1.2-1 Flow of Hardware Failure Recovery Confirmation

Copyright © 2014, 2017, Hitachi, Ltd.

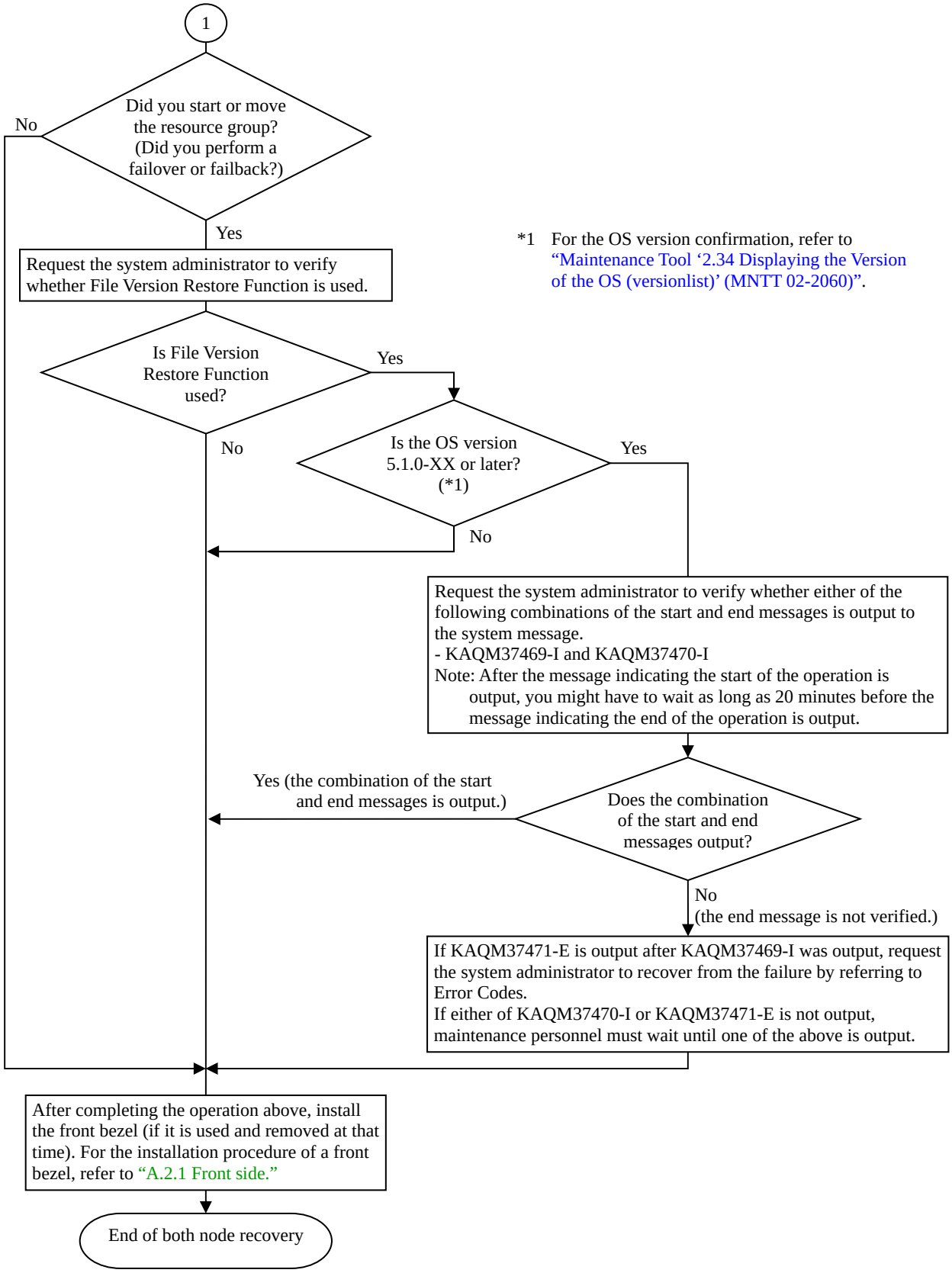


Figure 9.1.2-1 Flow of Hardware Failure Recovery Confirmation (2/2)

Copyright © 2014, 2018, Hitachi, Ltd.

9.1.2.1 Confirmation of hardware configuration and hardware normal status within node

Check if all of the hardware within the both nodes are in normal status using "hwstatus" command.

Check if the hardware output results (items of Fan Information, Temperature Information, Power Supply Information, Memory Information, Internal HDD Information, Internal RAID Battery Information, and BMC Information) are “OK” or “installed.” For Network Interface items, check if mng0, hb0, pm0, pm1 (*2) and ethX (*1), xgbeX (*1) are “UP”.

*1: Provided that the cable is connected. The value of “X” is an integer 0 or greater.
*2: Check only when the BMC direct connection configuration.

For the details about output result of hwstatus command, refer to “B.3.1.2 Output format”.

A part of Network Interface Card might not be able to perform I/O to the system even if Network Interface Card can link up by Link-up LED or the hwstatus command. In this case, contact the Technical Support Division.

Even if you confirmed that a node does not have a failure on D51B-2U, fault LED on the node might be lit. However it does not have a problem.

Copyright © 2014, 2015, Hitachi, Ltd.

9.1.2.2 Confirmation of FC path normal status

Check if all of the FC path within the both nodes are in normal status using "fpstatus" command.

Figure 9.1.2.2-1 shows an example of output result of the fpstatus command execution (on the node0 side). Check if all of the FC path are in "Online" status.

```
$ sudo fpstatus -v
Path                Target    HostPort HostPortWWN      ArrayPort  ArrayPortWWN     Model  Serial     Status
path000-0004-0A N0-T000   fc0004   10000000c98f26be 0A         50060e800044b632 AMS    87010001 Online
path000-0006-1A N0-T000   fc0006   10000000c98f36be 1A         50060e800044b636 AMS    87010001 Online
path001-0004-0B N0-T001   fc0004   10000000c98f26be 0B         50060e8005271c72 AMS    87010001 Online
path001-0006-1B N0-T001   fc0006   10000000c98f36be 1B         50060e8005271c76 AMS    87010001 Online
```

Figure 9.1.2.2-1 Example of Output Result of the fpstatus Command (on the node0 Side)

For details about the output result of the fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

Copyright © 2014, Hitachi, Ltd.

9.1.3 Recovery Procedure for Software Failure

This section describes the failure recovery procedure and the final recovery procedure for a software failure which occurred during operation of Hitachi Data Ingestor.

Table 9.1.3-1 shows the acquired failure information, the status of Hitachi Data Ingestor, and the section to be referred to for action to be taken (the failure recovery procedure and the final recovery procedure) when a SIM message of software failure is issued. Execute the troubleshooting in reference to the Table 9.1.3-1.

NOTE:
- If more than one of SIMs including KAQK39500-E Detail=00 00 00 03 Level=00 Type=02 (cluster management LU file system blocked SIM) are displayed, give the priority to execute the recovery procedure of the cluster management LU file system blocked SIM.
- The following products are indicated with abbreviations shown on the right to ":".
  Hitachi Data Ingestor : HDI
  Hitachi File Services Manager : HFSM

Table 9.1.3-1 List of Software-related Failures (1/4)

#	SIM	Failure	Acquired failure information		HDI status		Recovery method	
			core file (*1)	Dump file	Use of failover	Service status	Failure recovery procedure	Final recovery procedure
1	KAQK39500-E Detail=00 00 00 02 Level=00 Type=02	User LU file system is blocked.	N	Y (*2)	Y (*3)	All or some services are stopped (*4)	9.1.3.1 Recovery from blockage of the user LU file system (TRBL 09-0080)	9.1.4 Upgrading the Software by Updating the OS Version (TRBL 09-0550)
2	KAQK39500-E Detail=00 00 00 03 Level=00 Type=02	Cluster management LU file system is blocked.	N	N	N	Service is running.	9.1.3.2 Recovery from blockage of the cluster management LU file system (TRBL 09-0240)	
3	KAQK39500-E Detail=00 00 04 04 Level=00 Type=0D	Failover consecutive occurrence failure (reset ping-pong inhibit operation)	N	Y (*2)	Repeat	Service is stopped.	9.1.3.1 Recovery from blockage of the user LU file system (TRBL 09-0080)	
4	KAQK39500-E Detail=00 00 00 06 Level=00 Type=02	Virtual Server system LU is blocked. (*5)	N	Y (*2)	Y	Some services are stopped	9.1.3.2.1 Recovery from blockage of the Virtual Server System LU (TRBL 09-0300)	

Legend: Y: Failure information is output. N: Failure information is not output.

*1: For the core file acquisition, refer to Troubleshooting "6.4 Core Files" (TRBL 06-0050).
*2: When the setting of Dump file collection is [--on], it collects the dump file. For details about the dump file refer to "Maintenance Tool '2.20 Setting whether to Collect Dumps (dumpset)' (MNTT 02-1360)".
*3: Existing or not existing of failover depends on the setting by the system administrator.
*4: Service is available for accesses to other than the blocked file system.
Execute the recovery procedure of failure that corresponds to each SIM. After the recovery procedure of failure, execute the final recovery process as soon as the measurement version of OS is obtained.
*5: HDI does not support Virtual Server.

Follow the failure recovery procedure corresponding to each SIM. After performing the failure recovery procedure, perform the final recovery procedure of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, Hitachi, Ltd.

Table 9.1.3-1 List of Software-related Failures (2/4)

#	SIM	Failure	Acquired failure information		HDI status		Recovery method	
			core file (*1)	Dump file	Use of failover	Service status	Failure recovery procedure	Final recovery procedure
5	KAQK39500-E Detail=00 02 00 02 Level=00 Type=0A	Mounting of file system to be stored the dump failed.	—	—	—	—	9.1.5 Software Recovery by Installing the OS Initially (TRBL 09-0600)	
6	KAQK39500-E Detail= 00 00 00 02 Level =00 Type=0c	The logical volume entered a state where it cannot be accessed. (The file system or differential-data snapshots can no longer be used.)	N	N (*2)	N (*3)	Some services are stopped. (*4)	Ask the system administrator to confirm whether KAQG51003-E message has been output in the system message. If the message has been output, confirm to system administrator that an appropriate action about KAQG51003-E has been finished. And acquire the trouble information and send it to the Technical Support Center. If the message has not been output, acquires the trouble information and send it to the Technical Support Center with the comment that "KAQG51003-E has not been output". To acquire the trouble information, refer to the Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000).	
7	KAQK39500-E Detail= 05 00 00 01 Level =00,Type=03	Memory image copying is complete successfully.	—	Y	Y	Service is running. Or some services are stopped.	Ask the system administrator to check the status of disk array subsystem to confirm whether there is a lack of pool space. If a there is a lack of pool space, report that the cause of the dump is a lack of pool space, and ask an expansion and recovery of the pool space. If there is no problem with the status of disk array subsystem, acquire the trouble information in reference to the Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000). Send the acquired information to the Technical Support Center and request the investigation of the trouble.	
8	KAQK39500-E Detail=Other than above	—	—	—	—	—	Acquire the trouble information in reference to the Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000). Send the acquired information to the Technical Support Center and request the investigation of the trouble.	

Legend: Y: Failure information is output. N: Failure information is not output.

*1: For the core file acquisition, refer to Troubleshooting "6.4 Core Files" (TRBL 06-0050).
*2: If the system administrator has finished the appropriate action, dump files might be created.
*3: If the system administrator has finished the appropriate action, failover might occur.
*4: If the system administrator has finished the appropriate action, the stopped service might start again.

Follow the failure recovery procedure corresponding to each SIM. After performing the failure recovery procedure, perform the final recovery procedure of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, 2017, Hitachi, Ltd.

NOTE: If more than one of SIMs including KAQK39505-E Detail=00 01 00 00 or KAQK39505-E Detail= 01 01 00 00 (cluster management LU failure SIM) are displayed, give the priority to execute the recovery procedure of the cluster management LU failure SIM.

Table 9.1.3-1 List of Software-related Failures (3/4)

#	SIM	Failure	Acquired failure information		HDI status		Recovery method	
			core file (*1)	Dump file	Use of failover	Service status	Failure recovery procedure	Final recovery procedure
9	KAQK39505-E Detail=00 01 00 00 or 01 01 00 00	Cluster management LU failure (when node service is started or stopped)	N	N	Y	All or some services are stopped.	9.1.3.3 Recovery from KAQK39505-E failure (TRBL 09-0310)	9.1.4 Upgrading the Software by Updating the OS Version (TRBL 09-0550)
	KAQK39505-E Detail=00 02 00 00 or 01 02 00 00	Failure in preprocessing the NFS sharing (when node service is started or stopped)						
	KAQK39505-E Detail=00 03 00 00 or 01 03 00 00	User LU failure (when node service is started or stopped)						
	KAQK39505-E Detail=00 04 00 00 or 01 04 00 00	Failure in setting/cancelling the NFS sharing (when node service is started or stopped)						
	KAQK39505-E Detail=00 05 00 00 or 01 05 00 00	Up/down failure of the virtual IP (when node service is started or stopped)						
	KAQK39505-E Detail=00 06 00 00 or 01 06 00 00	Failure in CIFS setting/cancelling (when node service is started or stopped)						
	KAQK39505-E Detail=00 08 00 00 or 01 08 00 00	Failure in start /stop of the resource group						
	KAQK39505-E Detail=00 0A 00 00 or 01 0A 00 00	File snapshot or file version restore function failure (when resource group is started or stopped) (*2)						
10	KAQK39505-E Detail=Other than above	—	—	—	—	—	Refer to Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000) and acquire the trouble information. Send the acquired information to the Technical Support Center and request the investigation of the trouble.	

*1: Refer to Troubleshooting "6.4 Core Files" (TRBL 06-0050) to get the core file.
*2: HDI does not support Snapshot.

Legend: Y: Failure information is output. N: Failure information is not output.

Follow the failure recovery procedure corresponding to each SIM. After performing the failure recovery procedure, perform the final recovery procedure of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, 2017, Hitachi, Ltd.

NOTE:
- If the SIM of KAQK39500-E or KAQK39505-E is also displayed, give the priority to execute the recovery procedure for the SIM.
- Since HDI does not support Virtual Server, KAQK39602-E is not output.
- If more than one of SIMs including KAQK39602-E Detail=00 00 01 10 Level=00 Type=04 or KAQK39602-E Detail 00 00 01 11 Level=00 Type=04 (Virtual Server file system mount/umount failure) are displayed, give the priority to execute the measurement procedure for the Virtual Server file system mount/umount failure.

Table 9.1.3-1 List of Software-related Failures (4/4)

#	SIM	Failure	Acquired failure information		HDI status		Recovery method
			core file (*1)	Dump file	Use of failover	Service status	Failure recovery procedure
11	KAQK39602-E Detail=00 00 01 10 Level=00 Type=04	Virtual Server file system mount failure	N	N	Y	All or some services are stopped.	9.1.3.4 Recovery from KAQK39602-E failure (TRBL 09-0540)
	KAQK39602-E Detail=00 00 01 11 Level=00 Type=04	Virtual Server file system umount failure					
	KAQK39602-E Detail=00 00 01 20 Level=00 Type=04	Failure in starting the NFS sharing					
	KAQK39602-E Detail=00 00 01 21 Level=00 Type=04	Failure in stopping the NFS sharing					
	KAQK39602-E Detail=00 00 01 30 Level=00 Type=04	Up failure of the virtual IP					
	KAQK39602-E Detail=00 00 01 31 Level=00 Type=04	Down failure of the virtual IP					
	KAQK39602-E Detail=00 00 01 40 Level=00 Type=04	Failure in CIFS starting					
	KAQK39602-E Detail=00 00 01 41 Level=00 Type=04	Failure in CIFS stopping					
	KAQK39602-E Detail=00 00 01 50 Level=00 Type=04	Failure in starting the File snapshot or the file version restore function					
	KAQK39602-E Detail=00 00 01 51 Level=00 Type=04	Failure in stopping the File snapshot or the file version restore function					
	KAQK39602-E Detail=00 00 01 F0 Level=00 Type=04	Failure in starting the resource group of Virtual Server					
	KAQK39602-E Detail=00 00 01 F1 Level=00 Type=04	Failure in stopping the resource group of Virtual Server					

*1: Refer to Troubleshooting “6.4 Core Files” (TRBL 06-0050) to get the core file.

Legend: Y: Failure information is output. N: Failure information is not output.

Follow the failure recovery procedure corresponding to each SIM. After performing the failure recovery procedure, perform the final recovery procedure of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, 2017, Hitachi, Ltd.

9.1.3.1 Recovery from blockage of the user LU file system

The failure recovery procedure and the recovery method for the blocked user LU file system are described below.

When a user LU file system is blocked, failure recovery method and procedure depends on the file system operation. The following failure recovery methods are available for the blocked user LU file system.

- Recovery by restoring the backup
- Recovery using the fsrepair command

Troubleshooting “Figure 9.1.3.1-1” (TRBL 09-0090) shows the flowchart to determine which from among the above four failure recovery methods is to be used.

For the final recovery procedure after performing the above recovery methods, refer to Troubleshooting “9.1.4 Upgrading the Software by Updating the OS Version” (TRBL 09-0550).

The flowchart of the failure recovery procedure shows the manner how the maintenance personnel cooperate with the system administrator to grasp the node system status.

Copyright © 2014, Hitachi, Ltd.

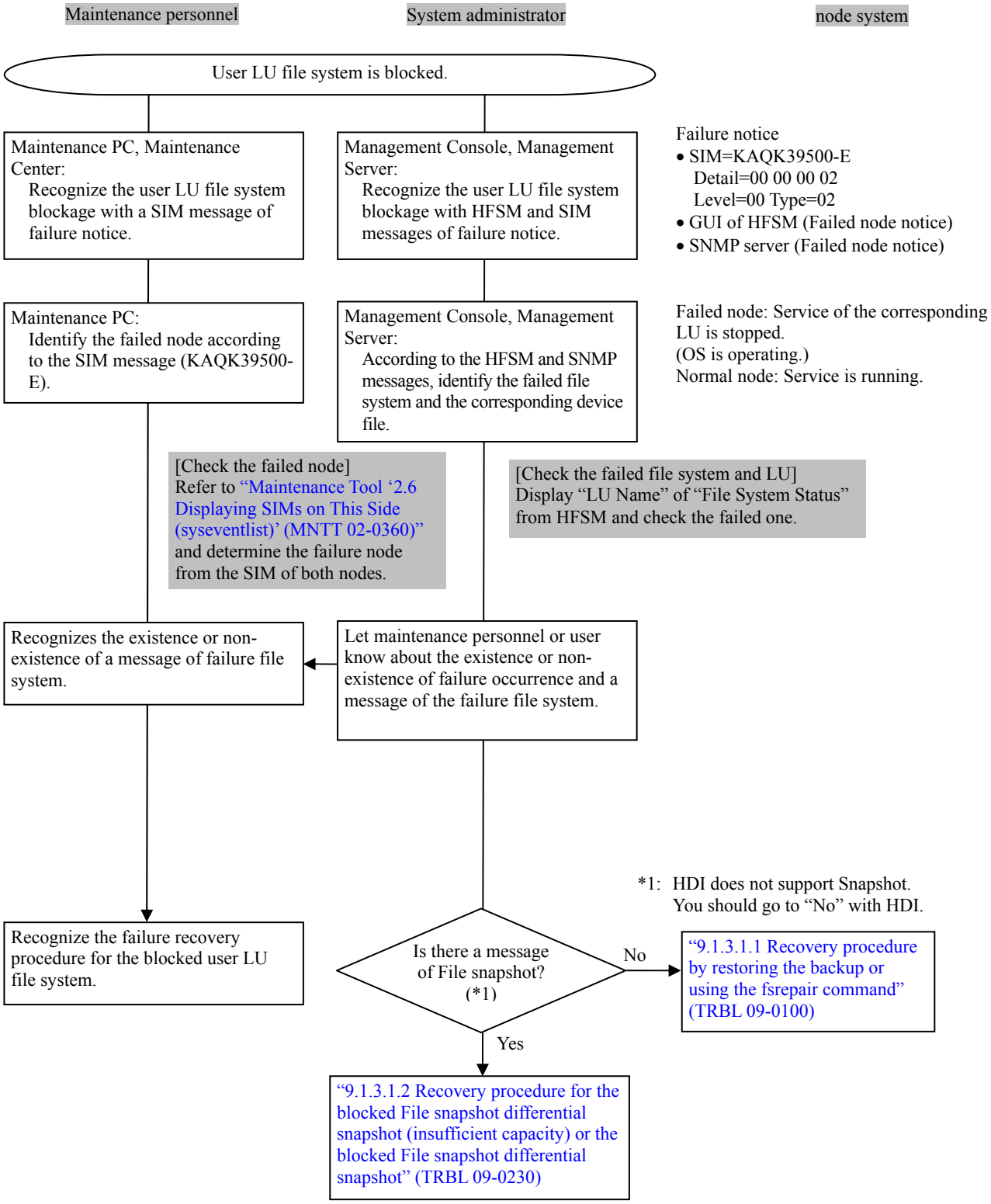


Figure 9.1.3.1-1 Determining the Recovery Method for the Blocked User LU File System

Copyright © 2014, 2017, Hitachi, Ltd.

9.1.3.1.1 Recovery procedure by restoring the backup or using the fsrepair command

This section describes the recovery procedure by restoring the backup or using the fsrepair command after occurrence of blockage of a user LU file system.

Table 9.1.3.1.1-1 shows the difference between the recovery procedure by restoring the backup and the recovery procedure using the fsrepair command.

Table 9.1.3.1.1-1 Difference between the Recovery Procedure by Restoring the Backup and the Recovery Procedure Using the fsrepair Command

Procedure	Procedure for recovery by restoring the backup	Procedure for recovery using the fsrepair command
1	Recognize a blocked user LU file system as a failure.	Recognize a blocked user LU file system as a failure.
2	Acquire the dump file manually.	Acquire the dump file manually.
3	Check that failover has been completed.	Check that failover has been completed.
4	Acquire the detailed information and send it to the Technical Support Center.	Acquire the detailed information and send it to the Technical Support Center.
5	Delete the failure file system.	Perform recovery of the failed file system.
6	Perform failback.	Perform failback.
7	Perform recreation and restoration of the failed file system.	—

Troubleshooting “Figure 9.1.3.1.1-1” (TRBL 09-0110) show the flowchart of the recovery procedure by restoring the backup and the recovery procedure using the fsrepair command. The flow is branched at the middle of the procedure into two: the recovery procedure by restoring the backup and the recovery procedure using the fsrepair command. Be careful of the difference and perform the recovery procedure.

After performing the failure recovery procedure, perform the final recovery procedure (Troubleshooting “9.1.4 Upgrading the Software by Updating the OS Version” (TRBL 09-0550)) of troubleshooting as soon as obtaining the update version of the OS.

When performing the file system recovery procedure with the fsrepair command, request the system administrator to be careful of the following notice.

NOTE:
- Execute the command operation via the management LAN.
- The fsrepair command may fail to recover the file system. If it fails, recover the file system from backup.
- If a wrong file system is attempted to be recovered, it may be destroyed. Be careful to select the file system encountered with a failure.
- When the fsrepair command is used to recover the file system, the user data which was updated just before the failure occurrence may not be reflected even though the integrity of the file system is recovered. If necessary, check the user data after recovery.

The flowchart of the failure recovery procedure shows the manner how the maintenance personnel cooperate with the system administrator to grasp the node system status.

Copyright © 2014, Hitachi, Ltd.

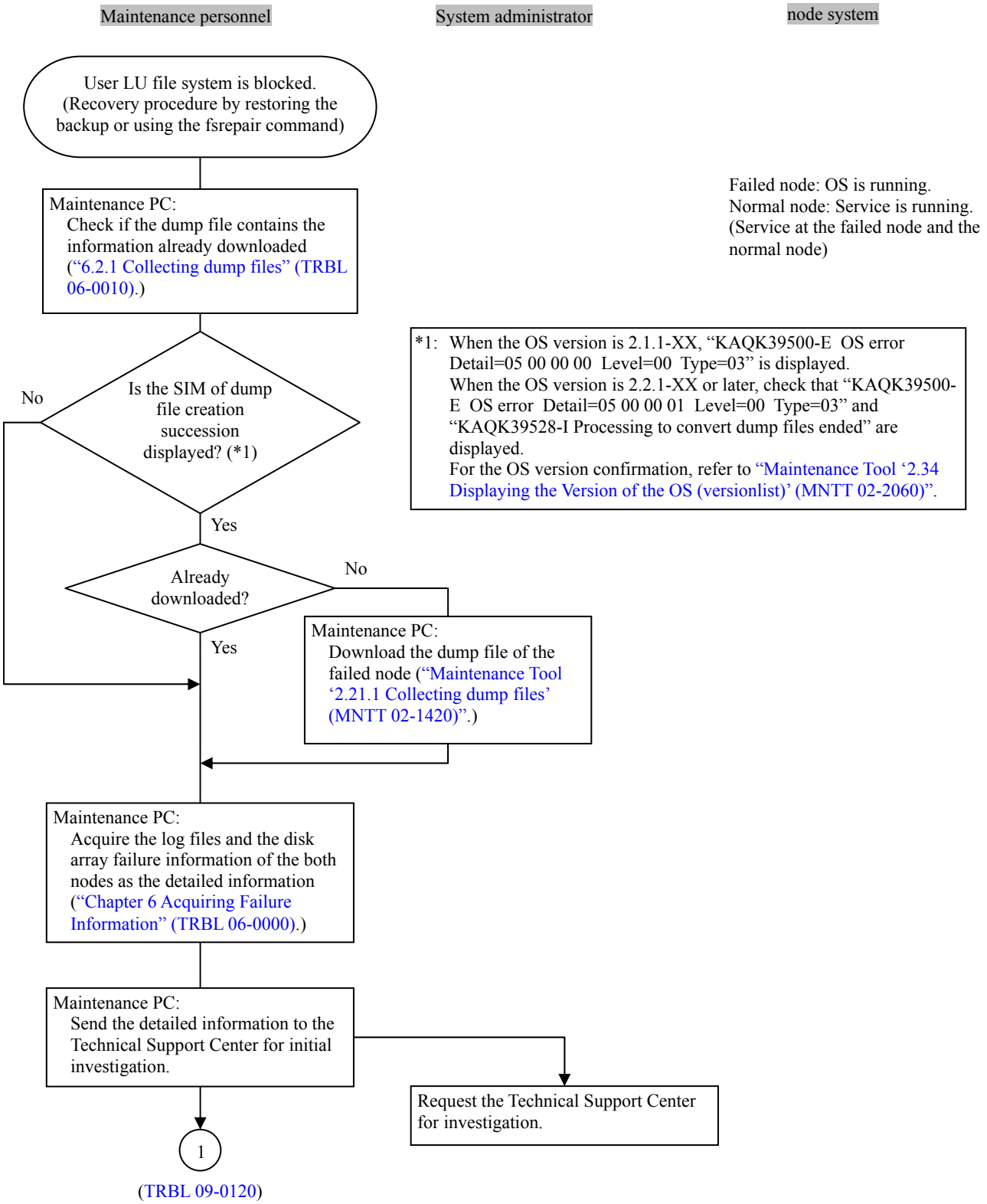


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (1/12)

Copyright © 2014, Hitachi, Ltd.

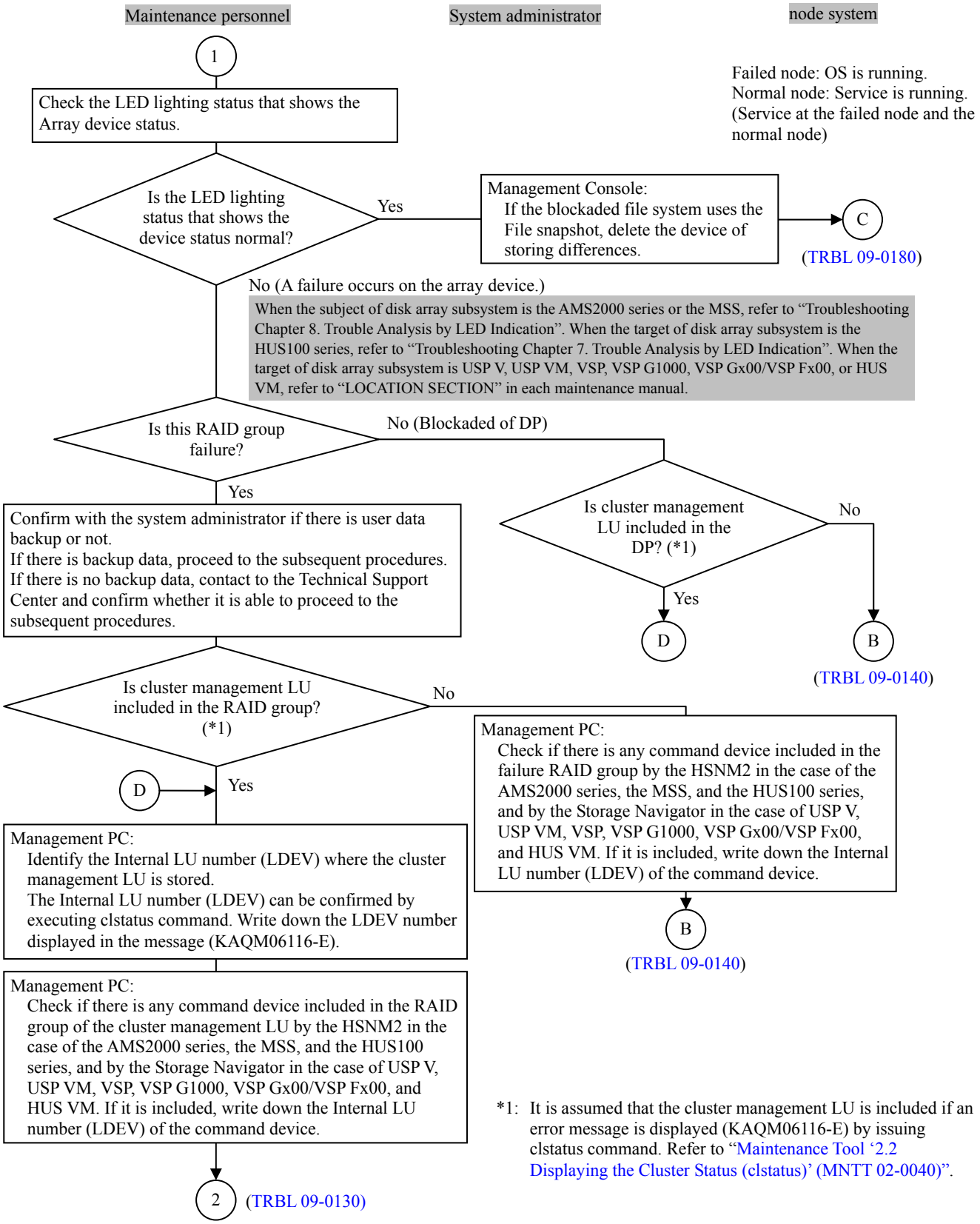


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (2/12)

Copyright © 2014, 2016, Hitachi, Ltd.

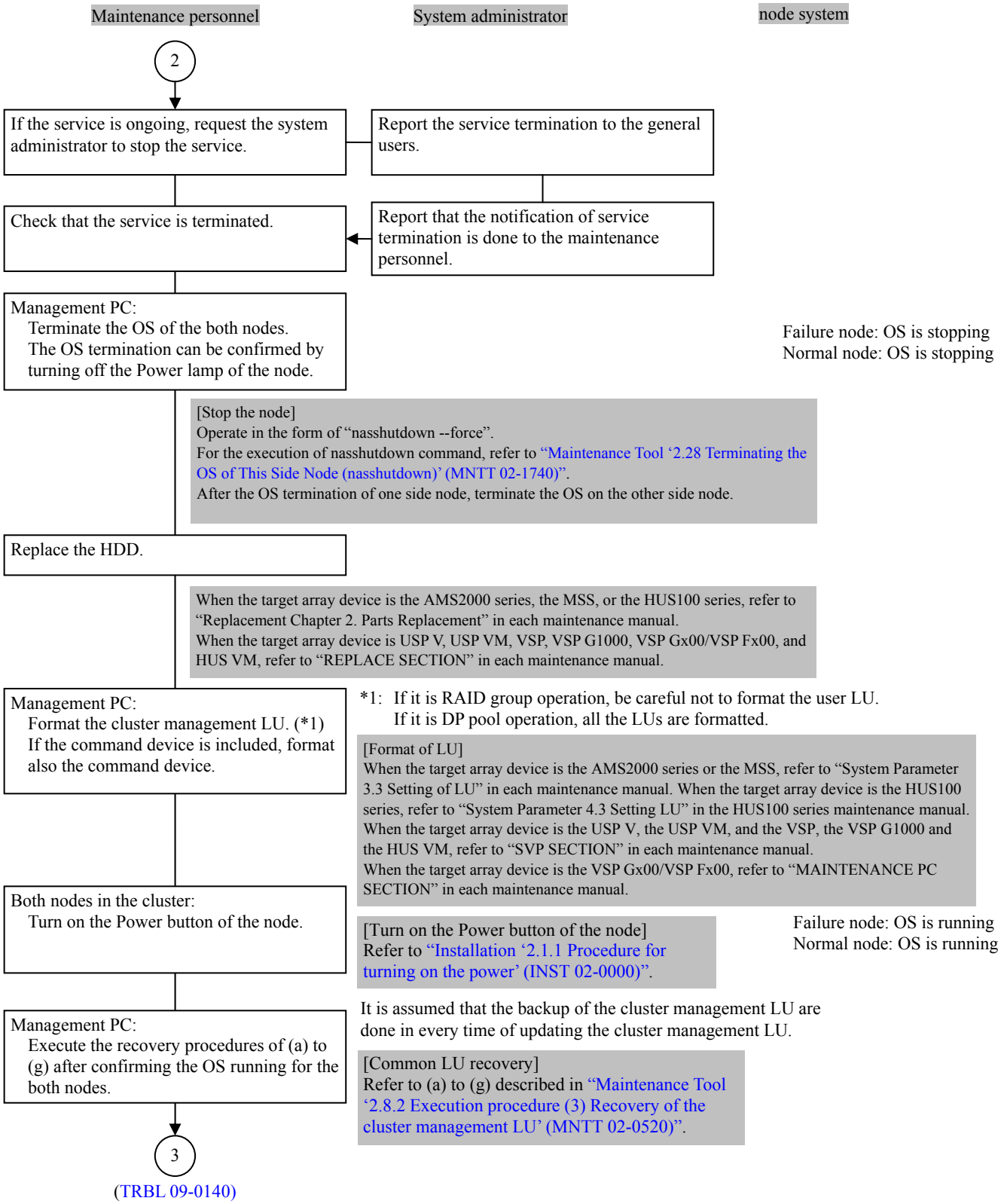


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (3/12)

Copyright © 2014, 2016, Hitachi, Ltd.

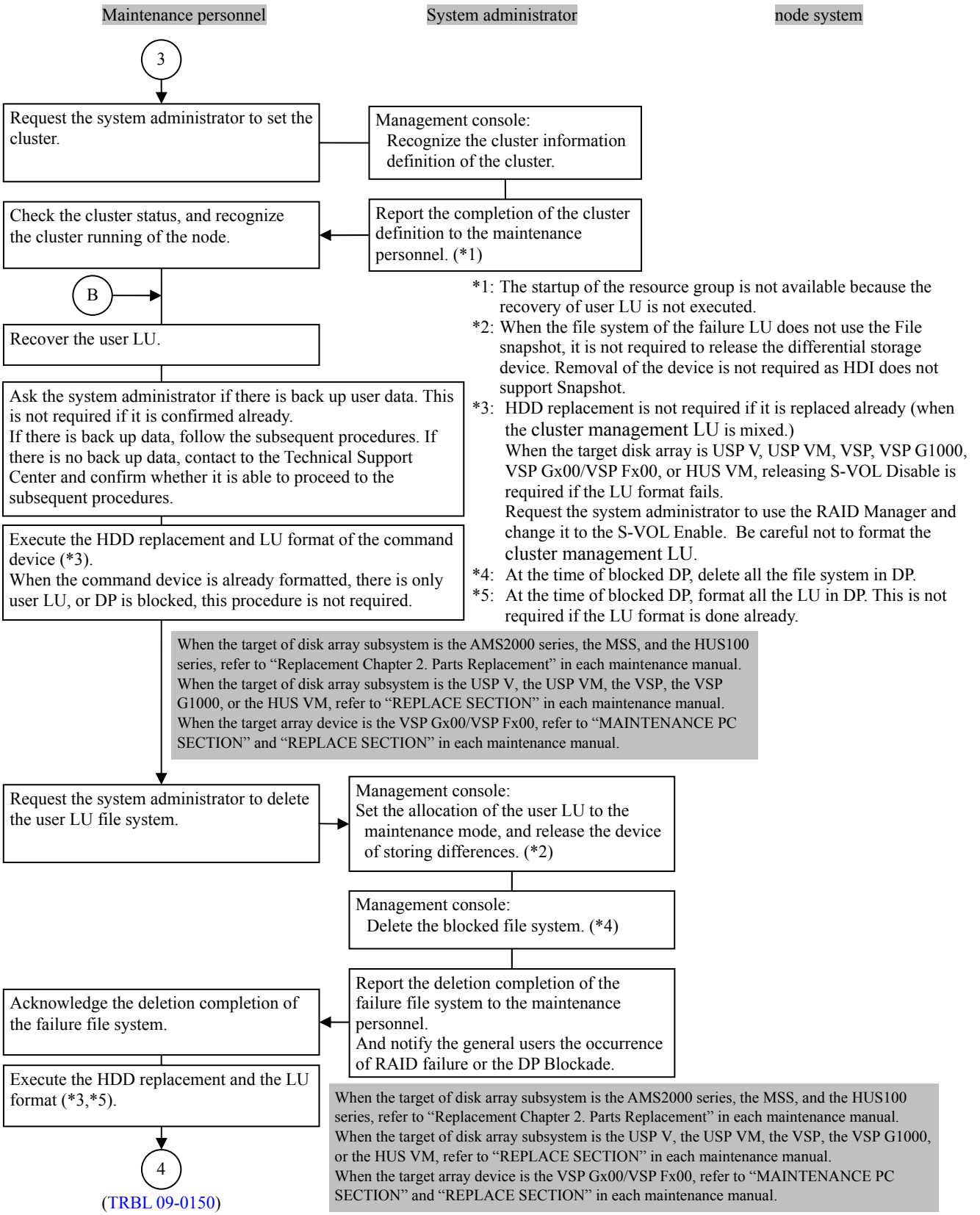


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (4/12)

Copyright © 2014, 2016, Hitachi, Ltd.

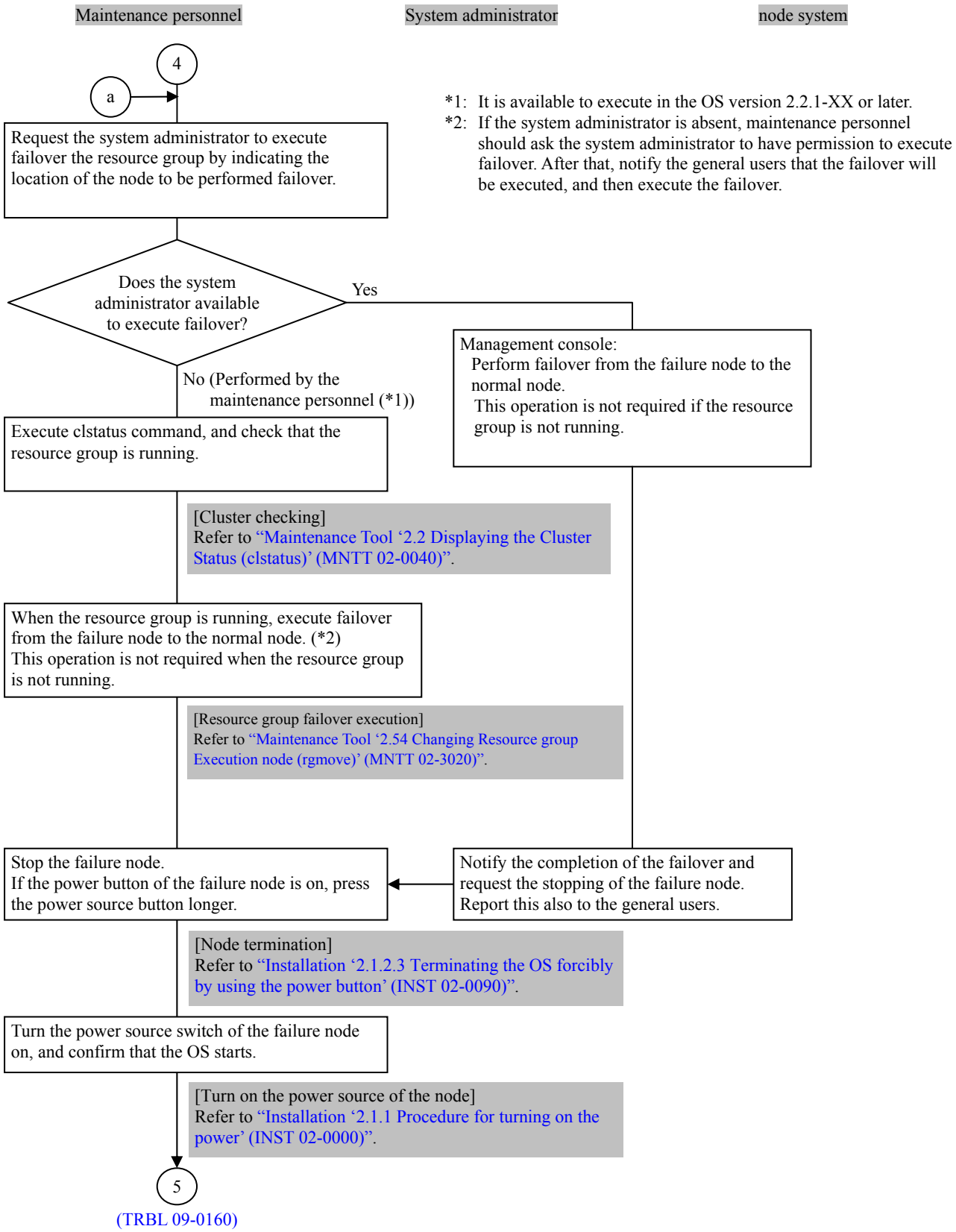


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (5/12)

Copyright © 2014, Hitachi, Ltd.

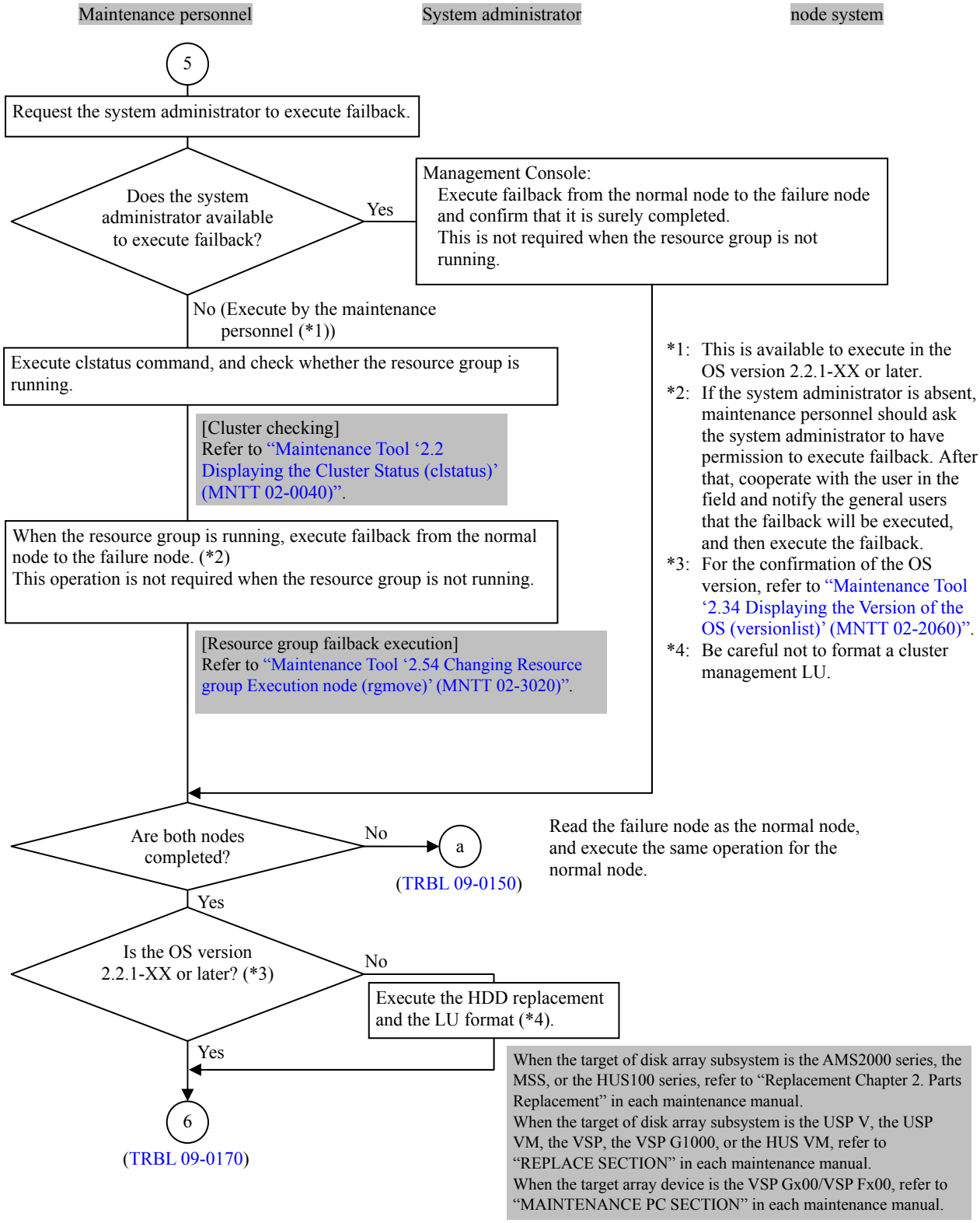


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (6/12)

Copyright © 2014, 2016, Hitachi, Ltd.

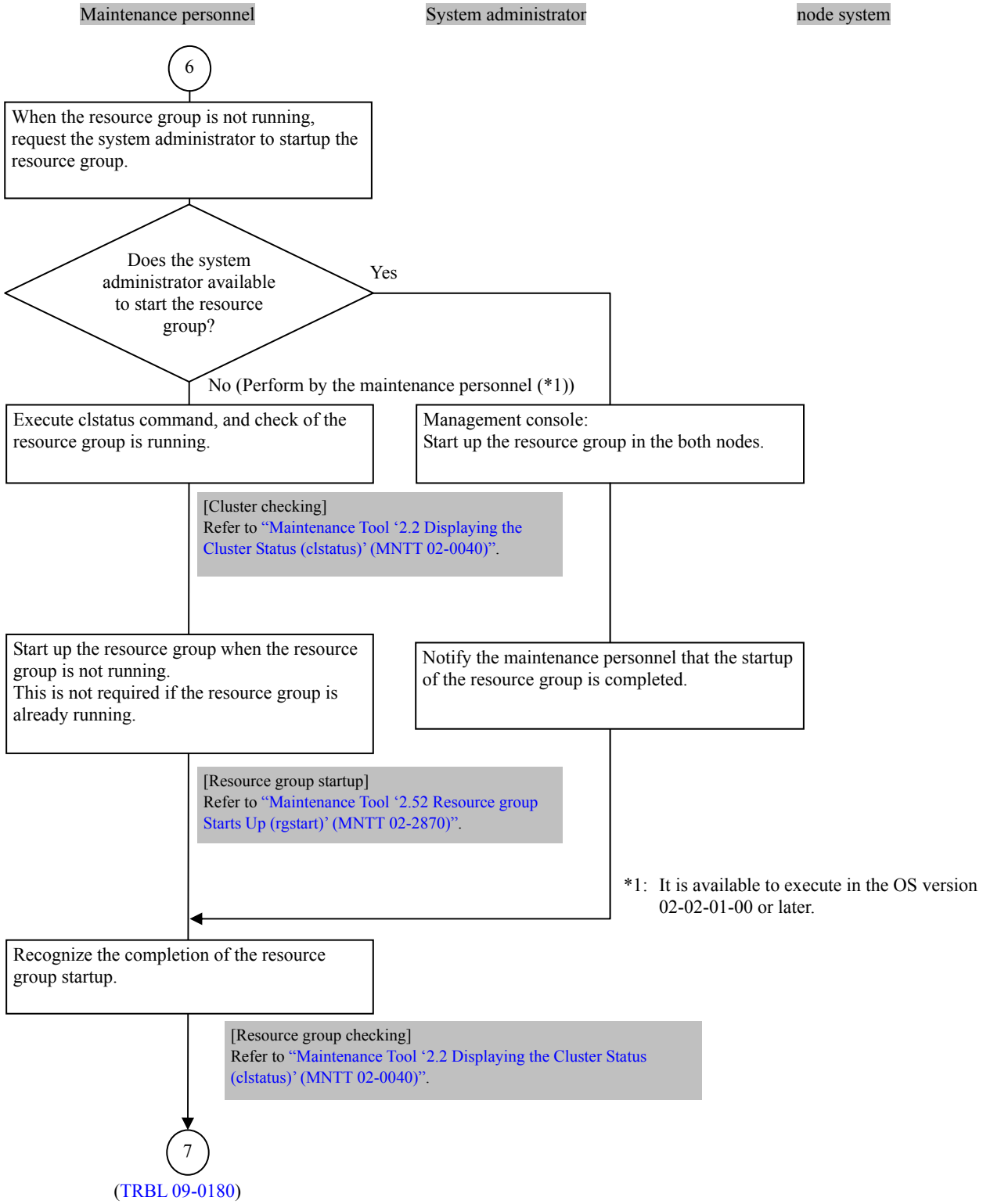
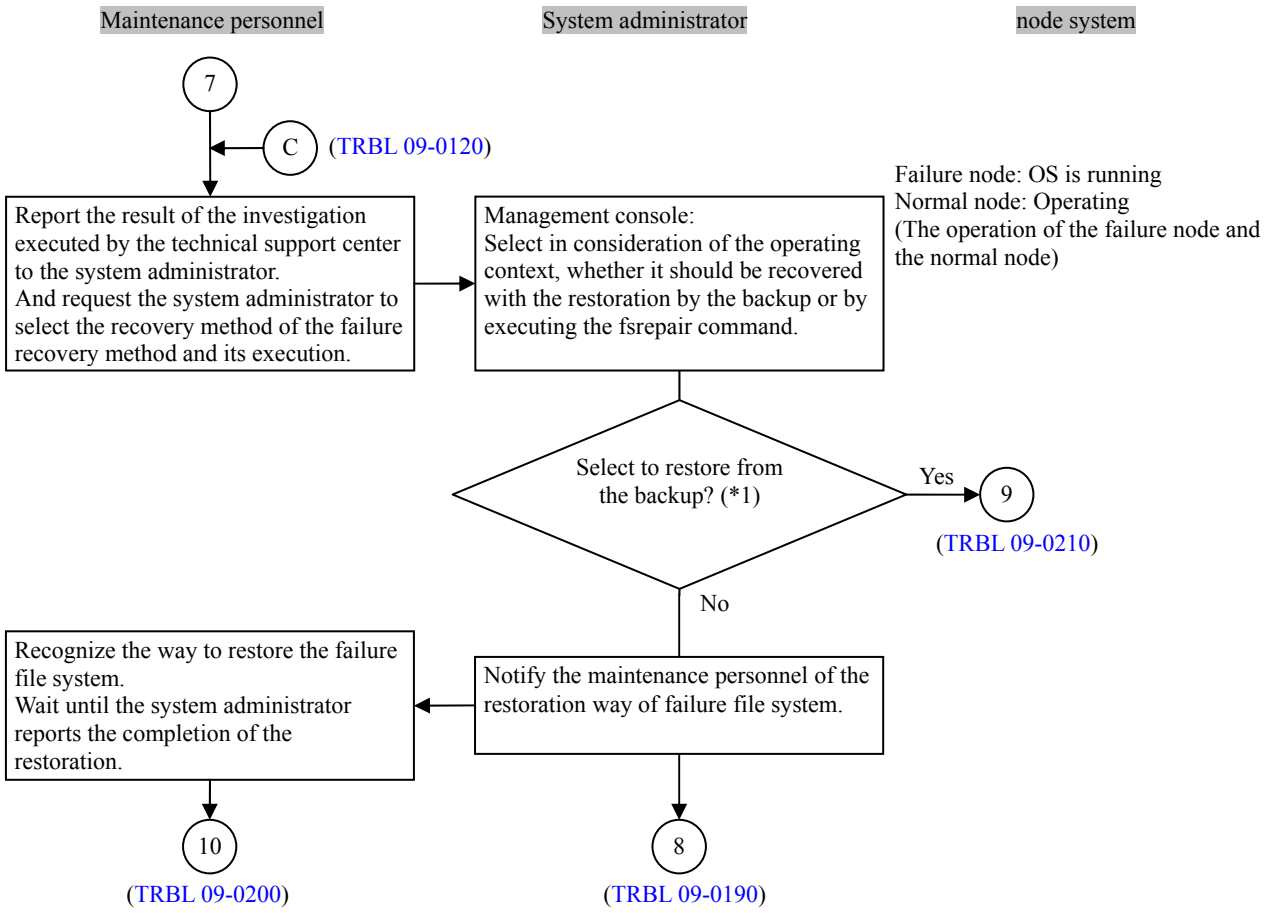


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (7/12)

Copyright © 2014, Hitachi, Ltd.



*1: Provide the following information to the system administrator, and follow his/her instruction.
- Recovery by executing restoration is to recreate the user file system and overwrite the backup data. Therefore, this method can only be recovered the file system status to the one that the date of backed up.
- Recovery by executing fsrepair command recovers the user file system before the occurrence of failures, by making match the file system integrity. However, destroyed data might not be recovered. It may take longer time for the recovery by the size of User LU and the number of files.
  Condition: 20,000,000 files in the state of no load.
  Time: (approx.) 2 hours.

NOTE:
- The restoration from the backup can only be done for the RAID failure.
- Execute the restoration from the backup when it is the configuration of HDI for Cloud.

Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (8/12)

Copyright © 2014, Hitachi, Ltd.

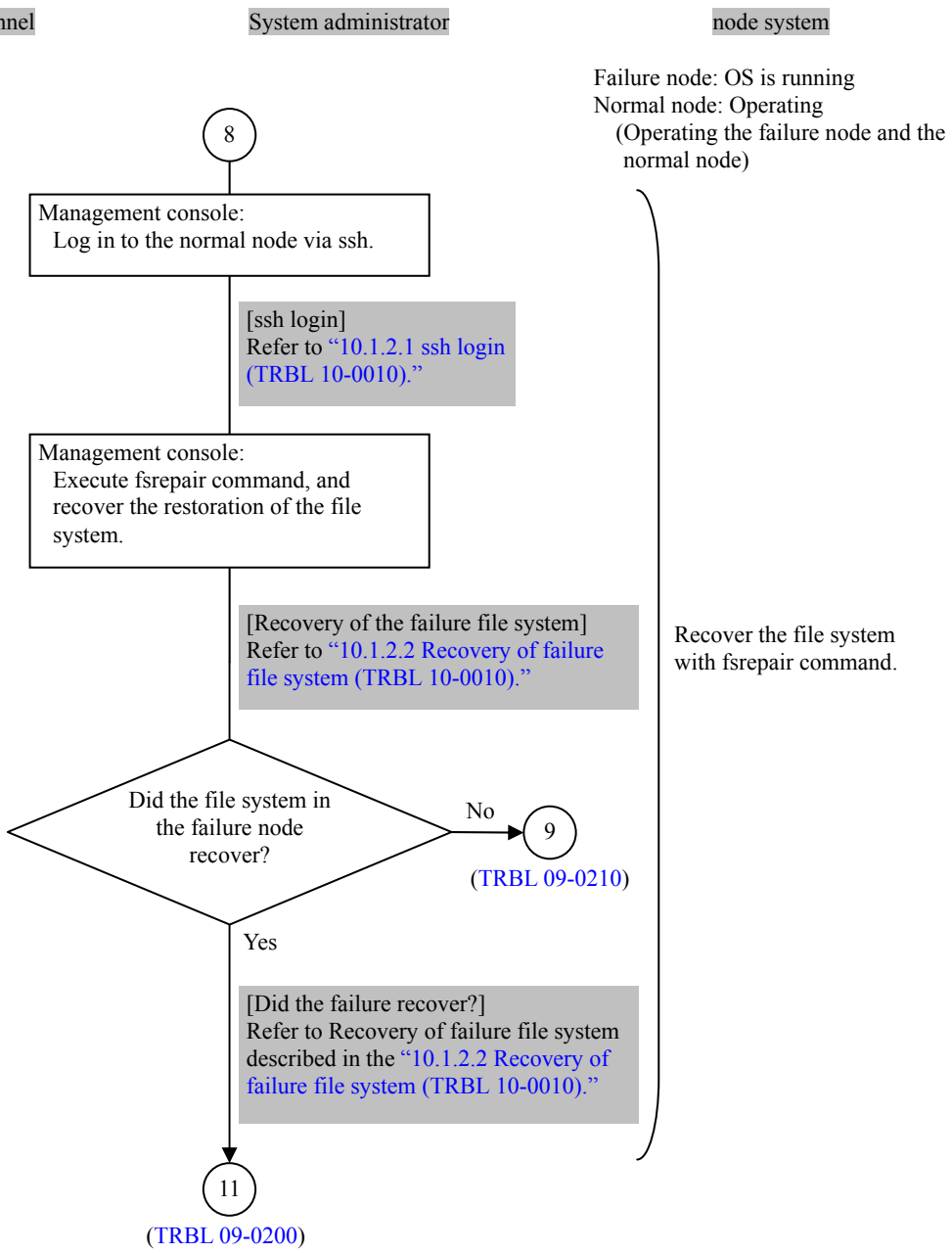


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (9/12)

Copyright © 2014, Hitachi, Ltd.

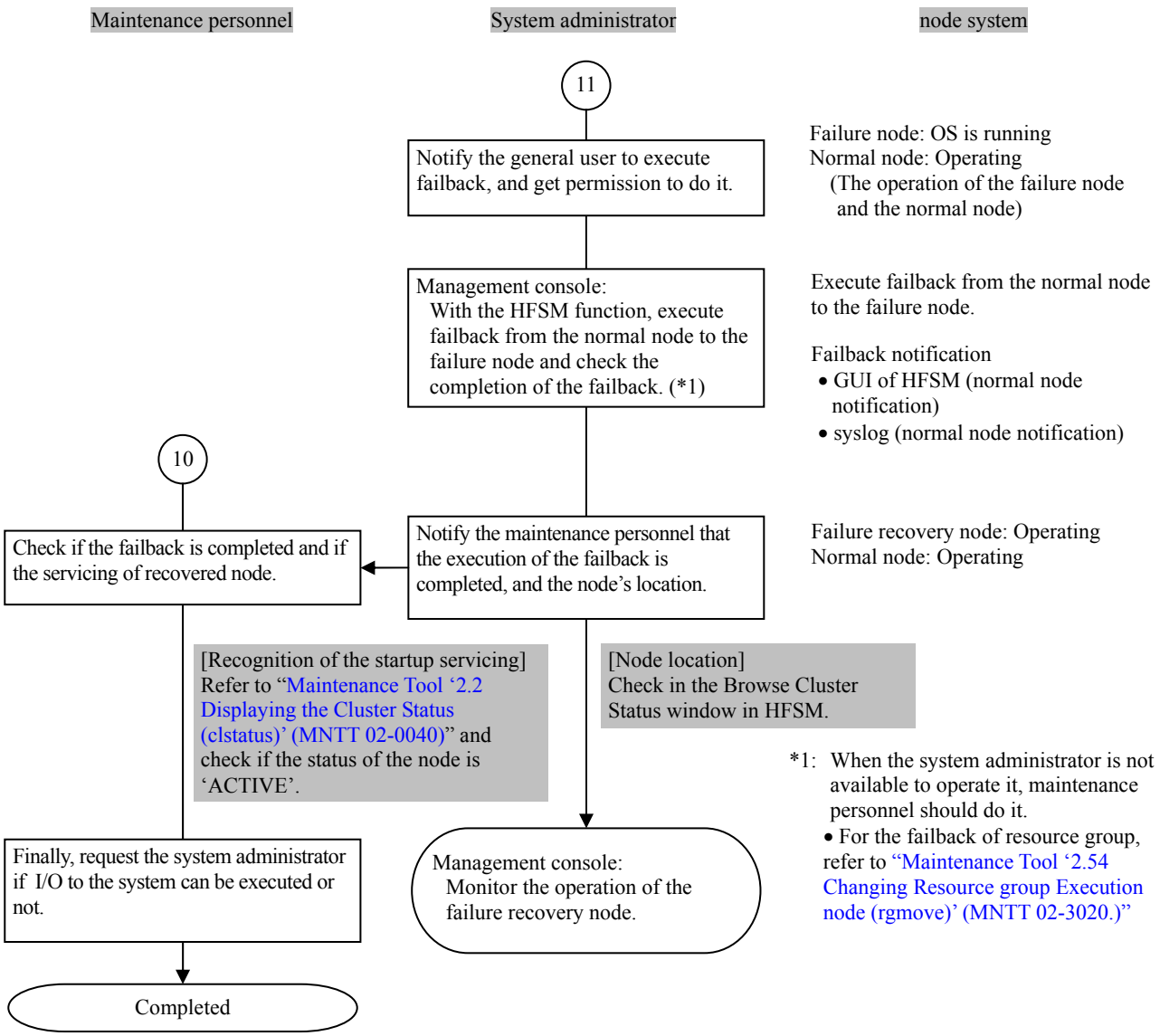


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (10/12)

Copyright © 2014, Hitachi, Ltd.

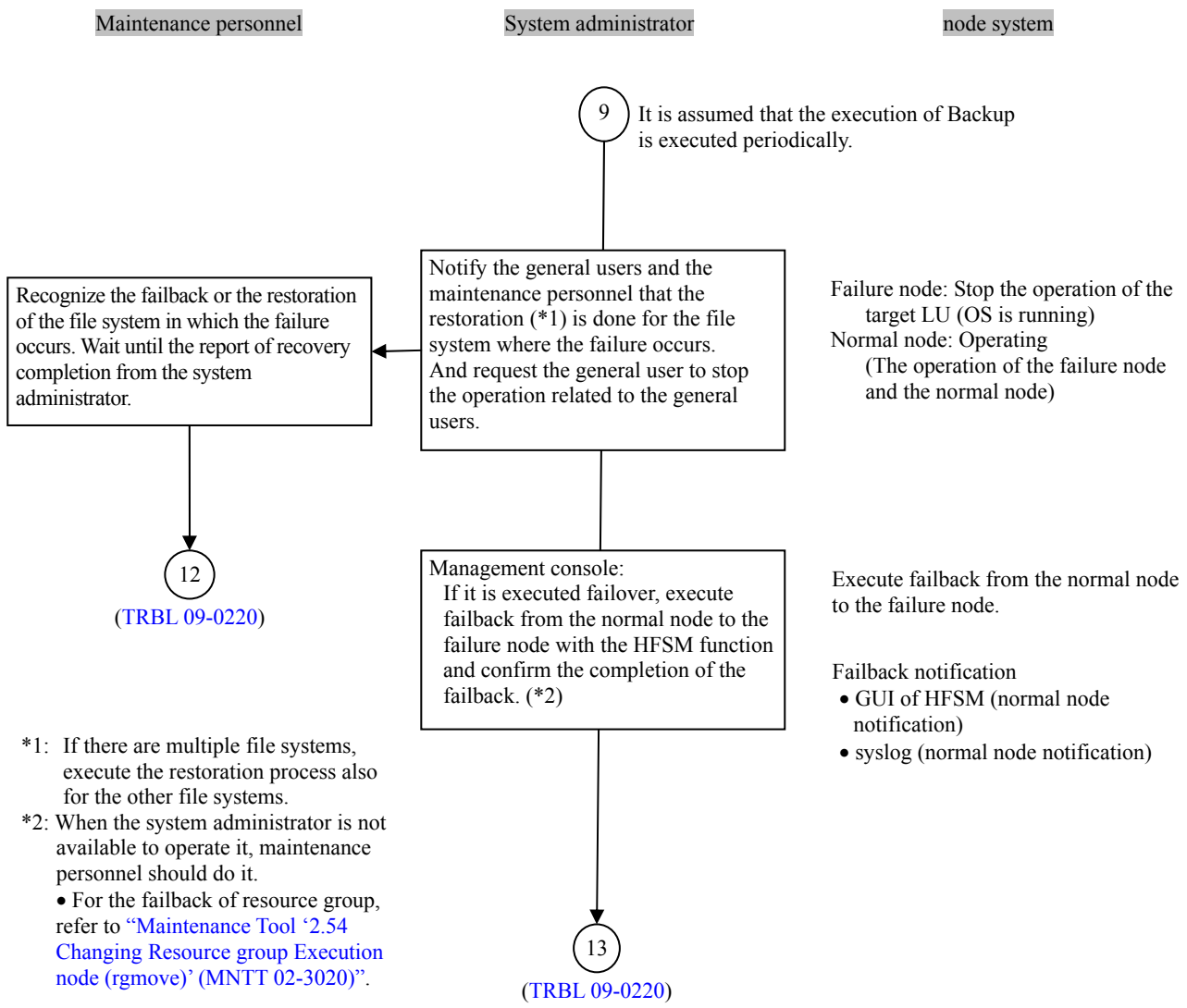


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (11/12)

Copyright © 2014, Hitachi, Ltd.

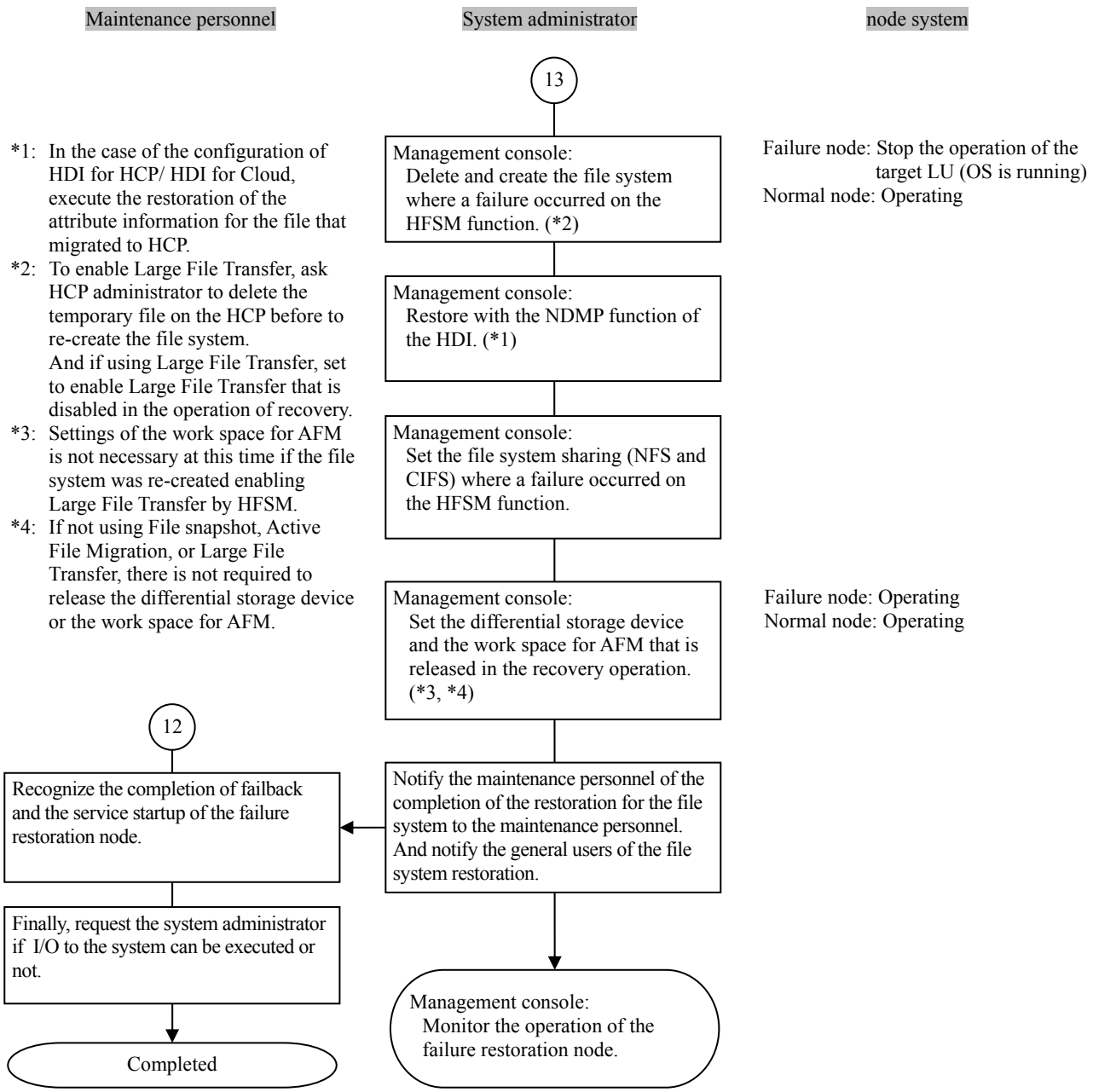


Figure 9.1.3.1.1-1 Recovery Procedure by Restoring the Backup or Using the fsrepair Command (12/12)

Copyright © 2014, 2017, Hitachi, Ltd.

9.1.3.1.2 Recovery procedure for the blocked File snapshot differential snapshot (insufficient capacity) or the blocked File snapshot differential snapshot

HDI does not support the Snapshot function.

Copyright © 2014, Hitachi, Ltd.

9.1.3.2 Recovery from blockage of the cluster management LU file system

NOTE: Rebooting nodes may recover the block of the cluster management LU caused by failures of disk array devices and the FC-SW. When referring to this procedure without isolating failures, be sure to execute "C.2.2.1 Failure Determination Procedure at the Cluster Configuration".

The failure recovery procedure and the recovery method for the blockage of the cluster management LU file system are described below.

Table 9.1.3.2-1 provides the overview of the recovery procedure for the cluster management LU file system blockage.

Table 9.1.3.2-1 Overview of the Recovery Procedure for the cluster management LU File System Blockage

Procedure	Recovery procedure	Remarks
1	Recognize that a failure occurred in the cluster management LU file system.	
2	Check whether a failure has occurred in the array subsystem.	If a failure has occurred, perform the failure determination.
3	Identify LDEV of the cluster management LU.	
4	Stop the OS and turn off the power buttons of both nodes.	
5	Formats the cluster management LU.	Be careful not to format a user LU.
6	Turn on the power buttons of both nodes.	If another system LU is recovered, the procedure up to here has already been executed.

Troubleshooting "Figure 9.1.3.2-1" (TRBL 09-0250) show the flowchart of the recovery procedure for blockage of the cluster management LU file system. Refer to the flow and execute the recovery procedure for the cluster management LU file system blockage.

After performing the failure recovery procedure, perform the final recovery procedure (Troubleshooting "9.1.4 Upgrading the Software by Updating the OS Version" (TRBL 09-0550)) of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, Hitachi, Ltd.

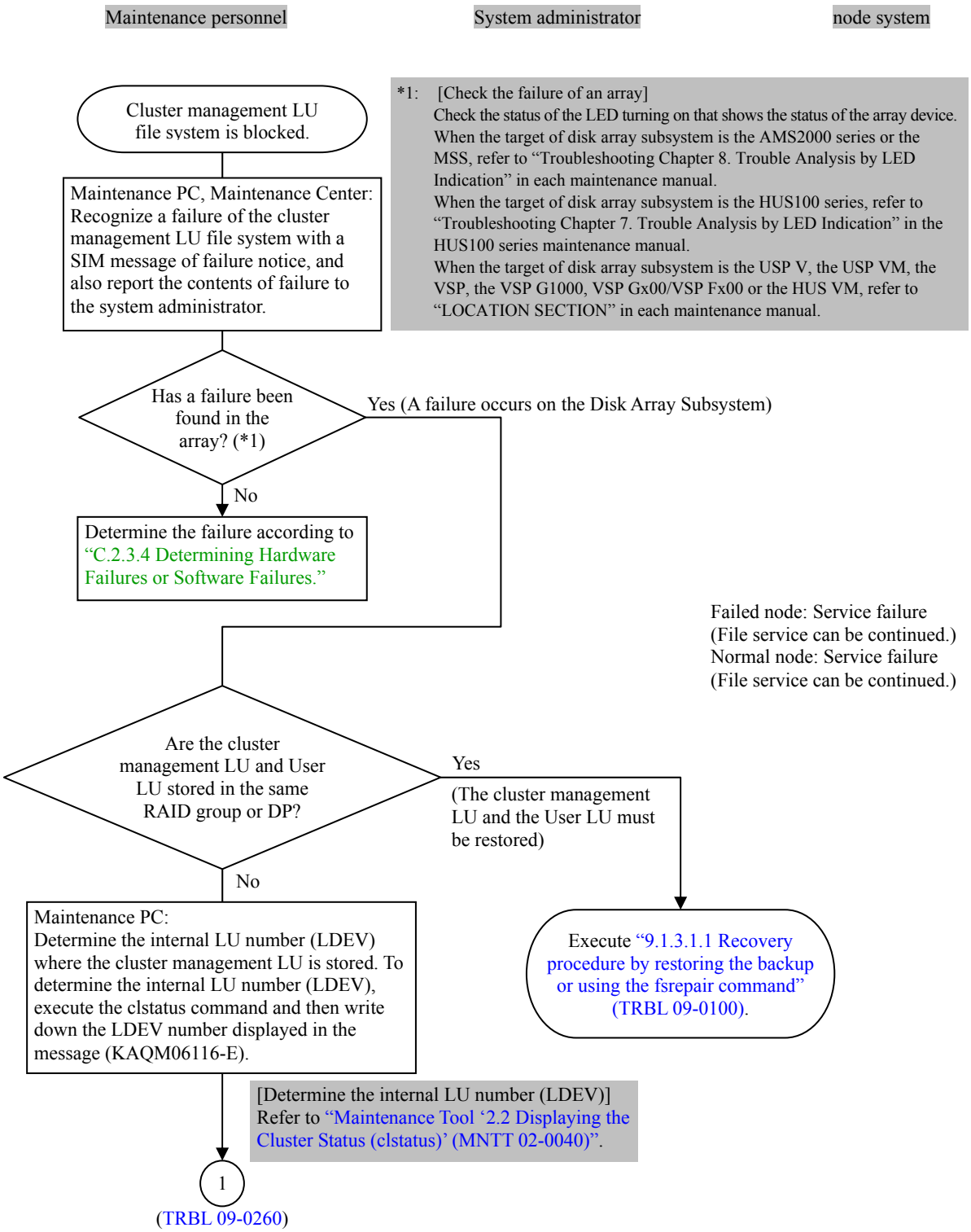


Figure 9.1.3.2-1 Recovery Procedure for Blockage of the Cluster management LU File System (1/5)

Copyright © 2014, 2016, Hitachi, Ltd.

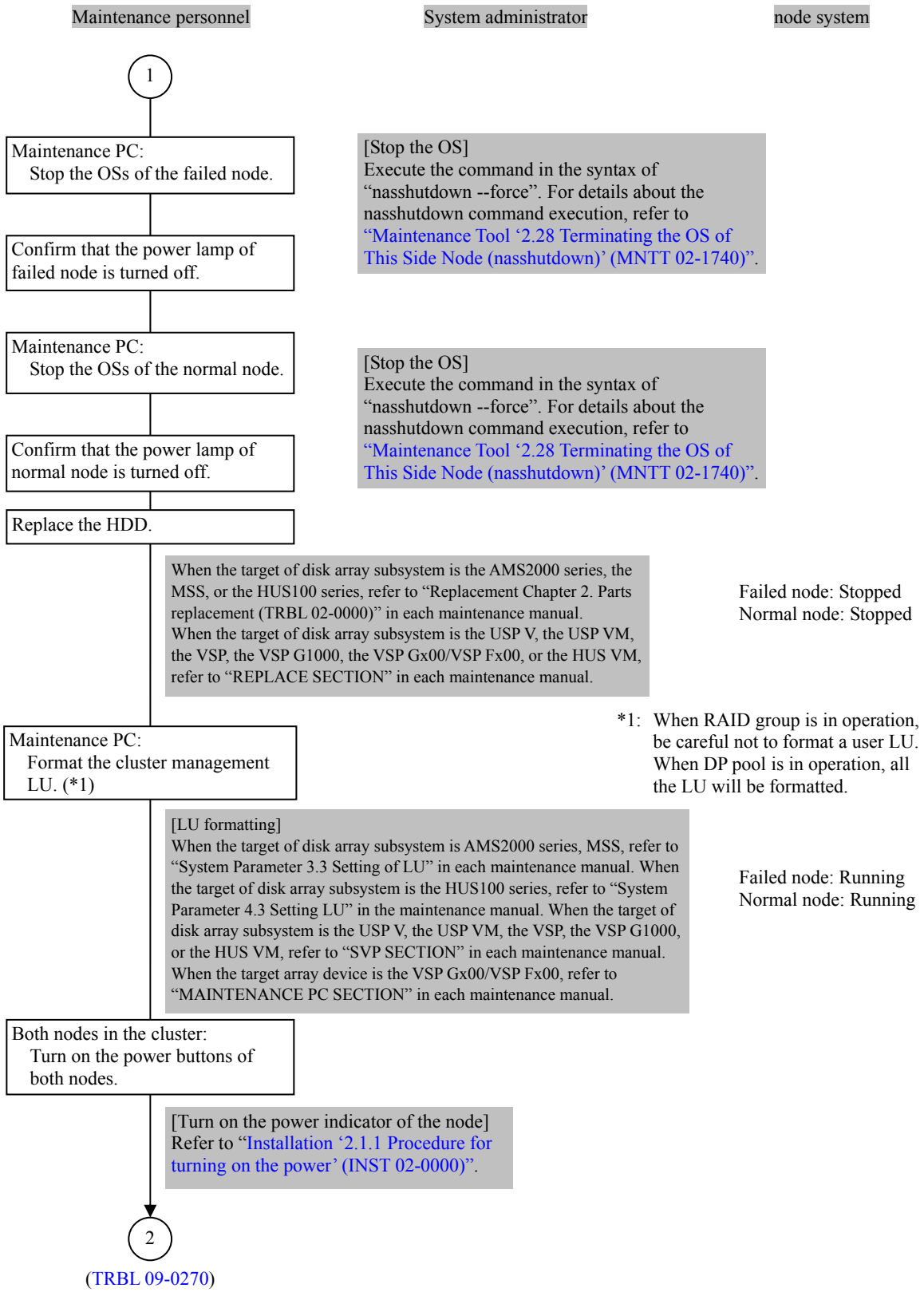
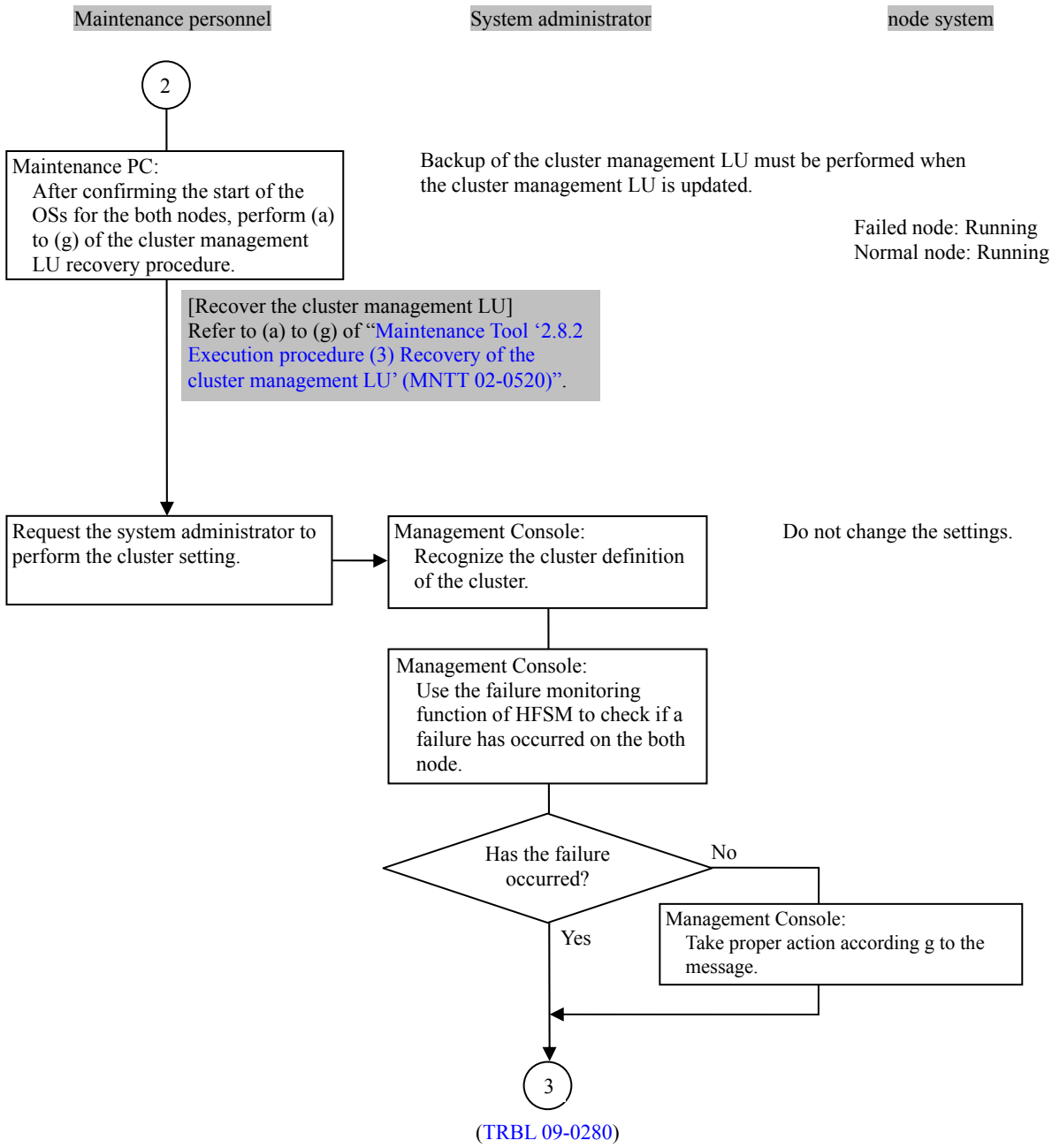


Figure 9.1.3.2-1 Recovery Procedure for Blockage of the Cluster management LU File System (2/5)

Copyright © 2014, 2016, Hitachi, Ltd.



(TRBL 09-0280)

Figure 9.1.3.2-1 Recovery Procedure for Blockage of the Cluster management LU File System (3/5)

Copyright © 2014, Hitachi, Ltd.

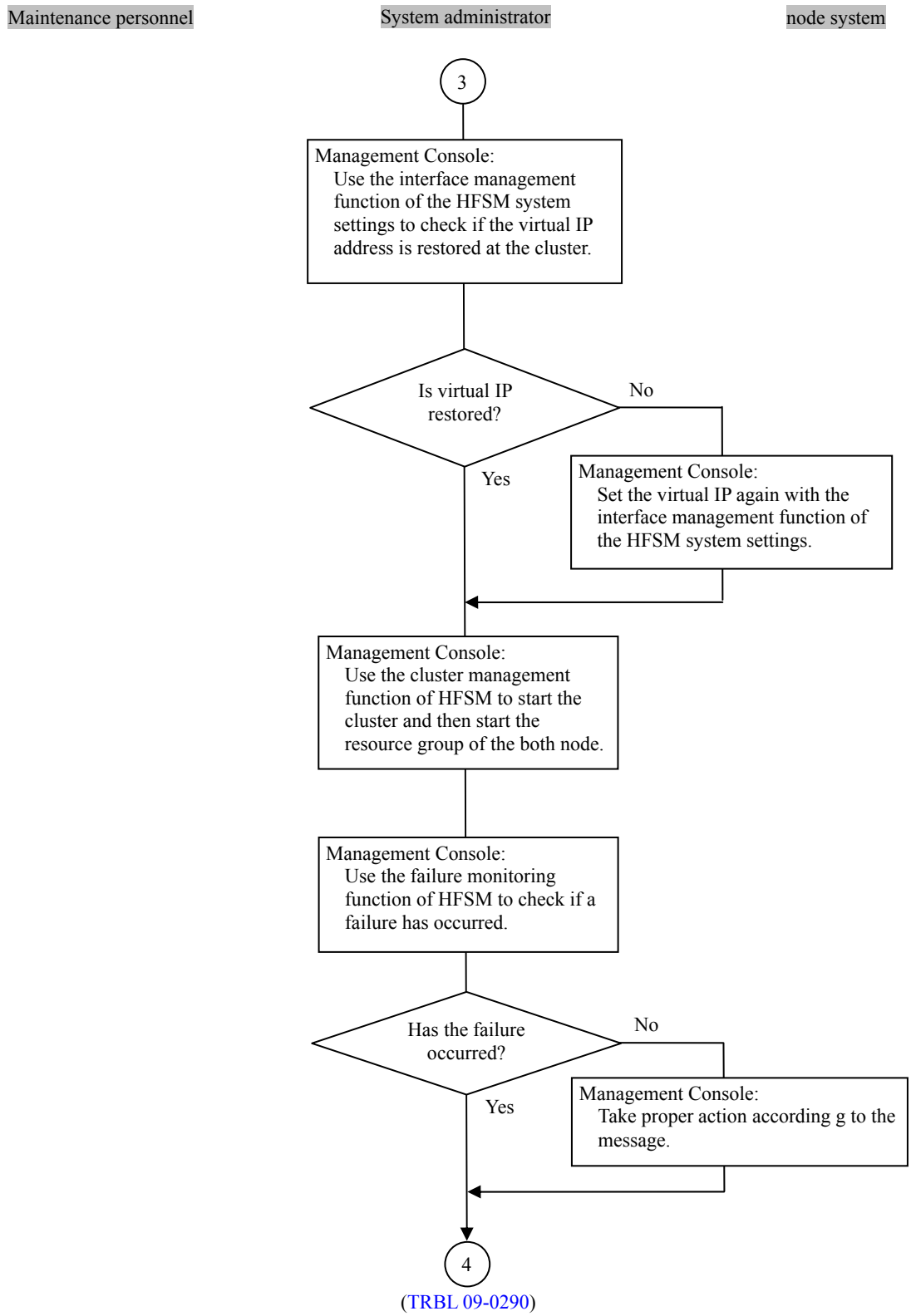


Figure 9.1.3.2-1 Recovery Procedure for Blockage of the Cluster management LU File System (4/5)

Copyright © 2014, Hitachi, Ltd.

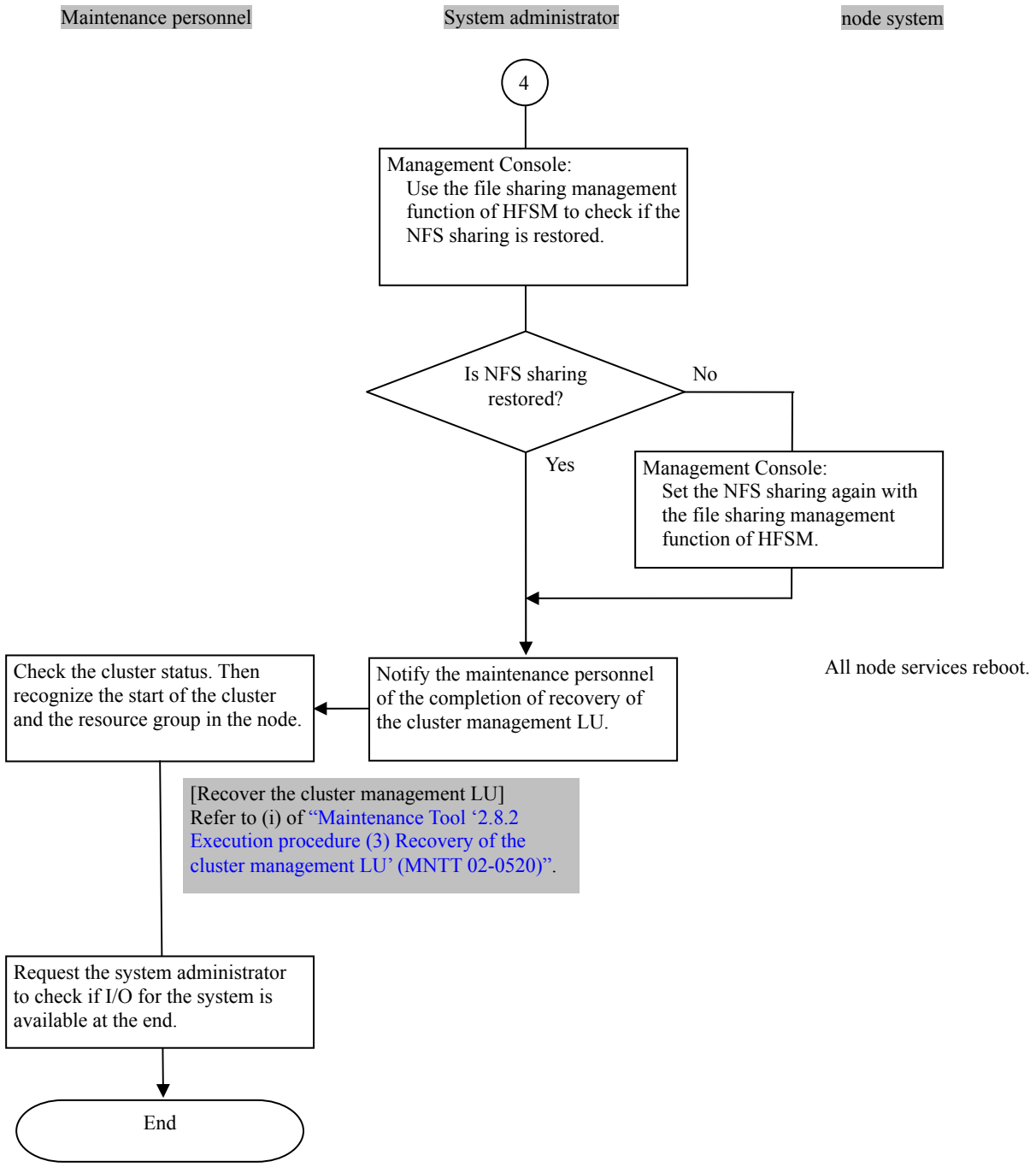


Figure 9.1.3.2-1 Recovery Procedure for Blockage of the Cluster management LU File System (5/5)

Copyright © 2014, Hitachi, Ltd.

9.1.3.2.1 Recovery from blockage of the Virtual Server System LU

HDI does not support Virtual Server.

Copyright © 2014, Hitachi, Ltd.

9.1.3.3 Recovery from KAQK39505-E failure

The failure recovery procedure and the recovery method corresponding to the KAQK39505-E message are described below.
The SIM message KAQK39505-E shows detail codes corresponding to different failures. Identify the failure content by referring to the detail code.
Table 9.1.3.3-1 describes the detail codes and failure details of the KAQK39505-E message. Also it shows the sections to be referred to for recovery procedure.

Table 9.1.3.3-1 Detail Codes of KAQK39505-E and Failure Content

#	SIM and detail code	Meaning	Failure Content	Recovery procedure (*2)
1	KAQK39505-E Detail=00 01 00 00	Mounting the cluster management LU failed (CLU partition failure).	Cluster management LU failure (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.2 (TRBL 09-0360)
	KAQK39505-E Detail=01 01 00 00	Unmounting the cluster management LU failed (CLU partition failure).		
2	KAQK39505-E Detail=00 02 00 00	Preprocessing of NFS failed.	Failure in preprocessing the NFS sharing (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.3 (TRBL 09-0370)
	KAQK39505-E Detail=01 02 00 00	Post-processing of NFS failed.		
3	KAQK39505-E Detail=00 03 00 00	Mounting the file system failed.	User LU failure (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.4 (TRBL 09-0390)
	KAQK39505-E Detail=01 03 00 00	Unmounting the file system failed.		
4	KAQK39505-E Detail=00 04 00 00	Starting the NFS sharing failed.	Failure in setting/cancelling the NFS sharing (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.5 (TRBL 09-0490)
	KAQK39505-E Detail=01 04 00 00	Stopping the NFS sharing failed.		
5	KAQK39505-E Detail=00 05 00 00	Bringing the virtual IP up failed.	Up/down failure of the virtual IP (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.6 (TRBL 09-0500)
	KAQK39505-E Detail=01 05 00 00	Bringing the virtual IP down failed.		
6	KAQK39505-E Detail=00 06 00 00	Starting CIFS failed.	Failure in CIFS setting/cancelling (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.7 (TRBL 09-0510)
	KAQK39505-E Detail=01 06 00 00	Stopping CIFS failed.		
7	KAQK39505-E Detail=00 08 00 00	scripts failure (resource group start processing failed)	Resource group start or stop processing failed.	• 9.1.3.3.1 (TRBL 09-0330)
	KAQK39505-E Detail=01 08 00 00	scripts failure (resource group stop processing failed)		
8	KAQK39505-E Detail=00 0A 00 00	File snapshot or file version restore function failure (resource group start processing failed) (*1)	File snapshot or file version restore function failure (when node service is started or stopped)	• 9.1.3.3.1 (TRBL 09-0330) • 9.1.3.3.8 (TRBL 09-0530)
	KAQK39505-E Detail=01 0A 00 00	File snapshot or file version restore function failure (resource group stop processing failed) (*1)		

*1: HDI does not support Snapshot.

Copyright © 2014, 2017, Hitachi, Ltd.

*2 Recovery procedure branches into several branches in Flow (A) of Troubleshooting “Figure 9.1.3.3.1-1” (TRBL 09-0330). After branching, proceed to a flowchart corresponding to the type of failure (9.1.3.3.2-1 to 9.1.3.3.8-1) and execute the recovery procedure according to the flowchart. When the recovery procedure of each flowchart is completed, return to Flow (B) of Troubleshooting “Figure 9.1.3.3.1-1” (TRBL 09-0330) to confirm the recovery.

For the final recovery after the recovery procedure of KAQK39505-E, perform the procedure of Troubleshooting “9.1.4 Upgrading the Software by Updating the OS Version” (TRBL 09-0550).

NOTE: Check if any of the #2, #4, #6, and #8 detail codes is output together with the #3 or #5 detail code. If the #3 or #5 detail code is output, perform the #3 or #5 recovery procedure.

The flowchart of the failure recovery procedure shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status.

Copyright © 2014, 2017, Hitachi, Ltd.

9.1.3.3.1 Procedure for KAQK39505-E failure recovery

The failure recovery procedure for the KAQK39505-E message is described below in the form of a flowchart.

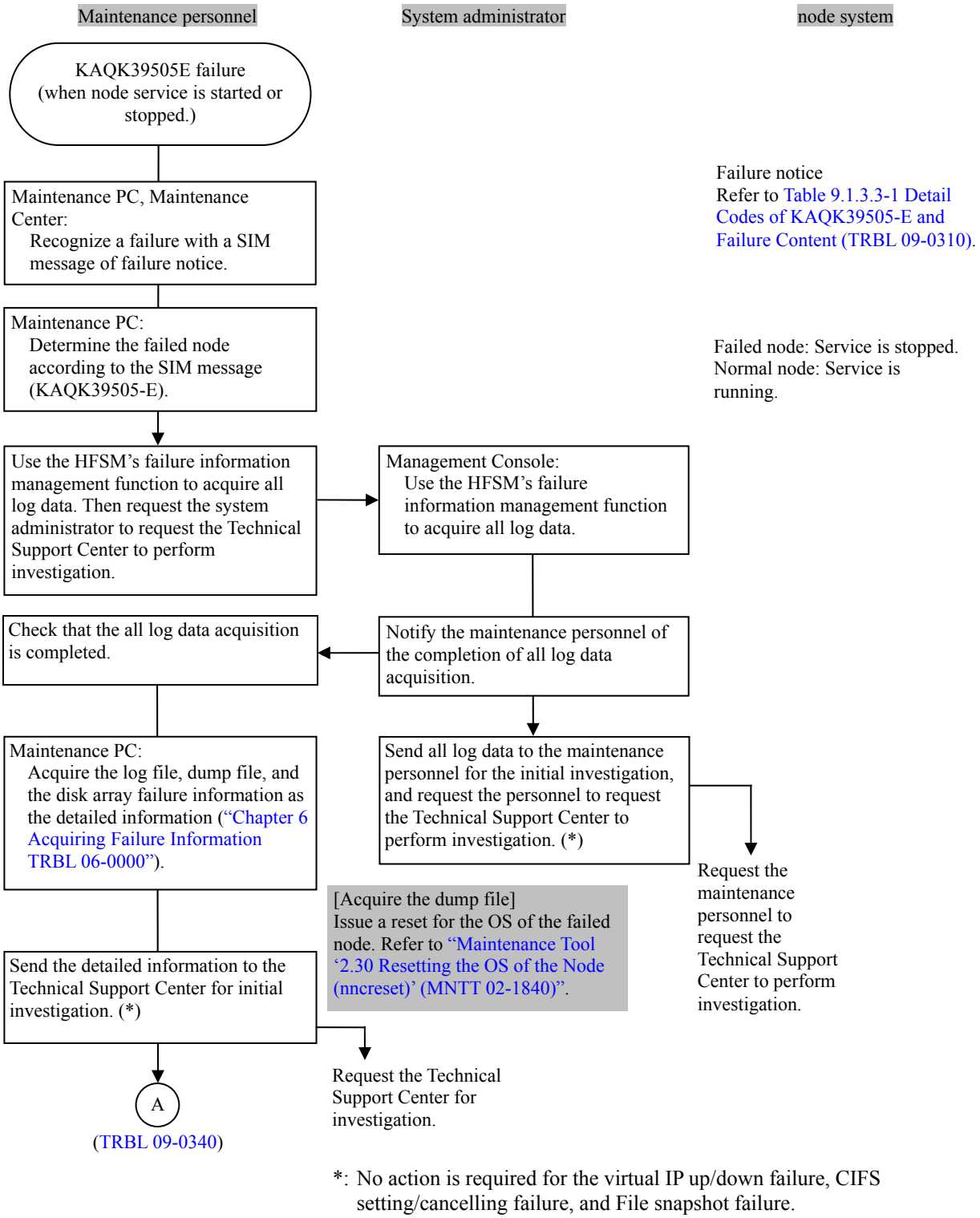


Figure 9.1.3.3.1-1 Procedure for KAQK39505-E Failure Recovery (1/3)

Copyright © 2014, Hitachi, Ltd.

Maintenance personnel | System administrator | node system

A

Perform any of the following failure recovery procedures (sections to be referred to) according to the failure content.

#	SIM and detail code	Failure Content	Next recovery procedure
1	KAQK39505-E Detail=00 01 00 00 or 01 01 00 00	Cluster management LU failure	9.1.3.3.2 (TRBL 09-0360)

When #1 is selected, the recovery procedure is completed in the referred-to section.

#	SIM and detail code	Failure Content	Next recovery procedure
2	KAQK39505-E Detail=00 02 00 00 or 01 02 00 00	Failure in preprocessing the NFS sharing	9.1.3.3.3 (TRBL 09-0370)
3	KAQK39505-E Detail=00 03 00 00 or 01 03 00 00	User LU failure	9.1.3.3.4 (TRBL 09-0390)
4	KAQK39505-E Detail=00 04 00 00 or 01 04 00 00	Failure in setting/cancelling the NFS sharing	9.1.3.3.5 (TRBL 09-0490)
5	KAQK39505-E Detail=00 05 00 00 or 01 05 00 00	Virtual IP up/down failure	9.1.3.3.6 (TRBL 09-0500)
6	KAQK39505-E Detail=00 06 00 00 or 01 06 00 00	Failure in CIFS setting/cancelling	9.1.3.3.7 (TRBL 09-0510)
7	KAQK39505-E Detail=00 08 00 00 or 01 08 00 00	Resource group processing failure	—
8	KAQK39505-E Detail=00 0A 00 00 or 01 0A 00 00	File snapshot or file version restore function failure	9.1.3.3.8 (TRBL 09-0530)

When any of #2 to #6, #8 is selected, return to “Procedure for KAQK39505-E Failure Recovery (3/3)” (TRBL 09-0350) on the next page after completing the recovery procedure of the referred-to section. #7 completes the recovery procedure by sending the failure information to the Technical Support Center.

B

(TRBL 09-0350)

Figure 9.1.3.3.1-1 Procedure for KAQK39505-E Failure Recovery (2/3)

Copyright © 2014, Hitachi, Ltd.

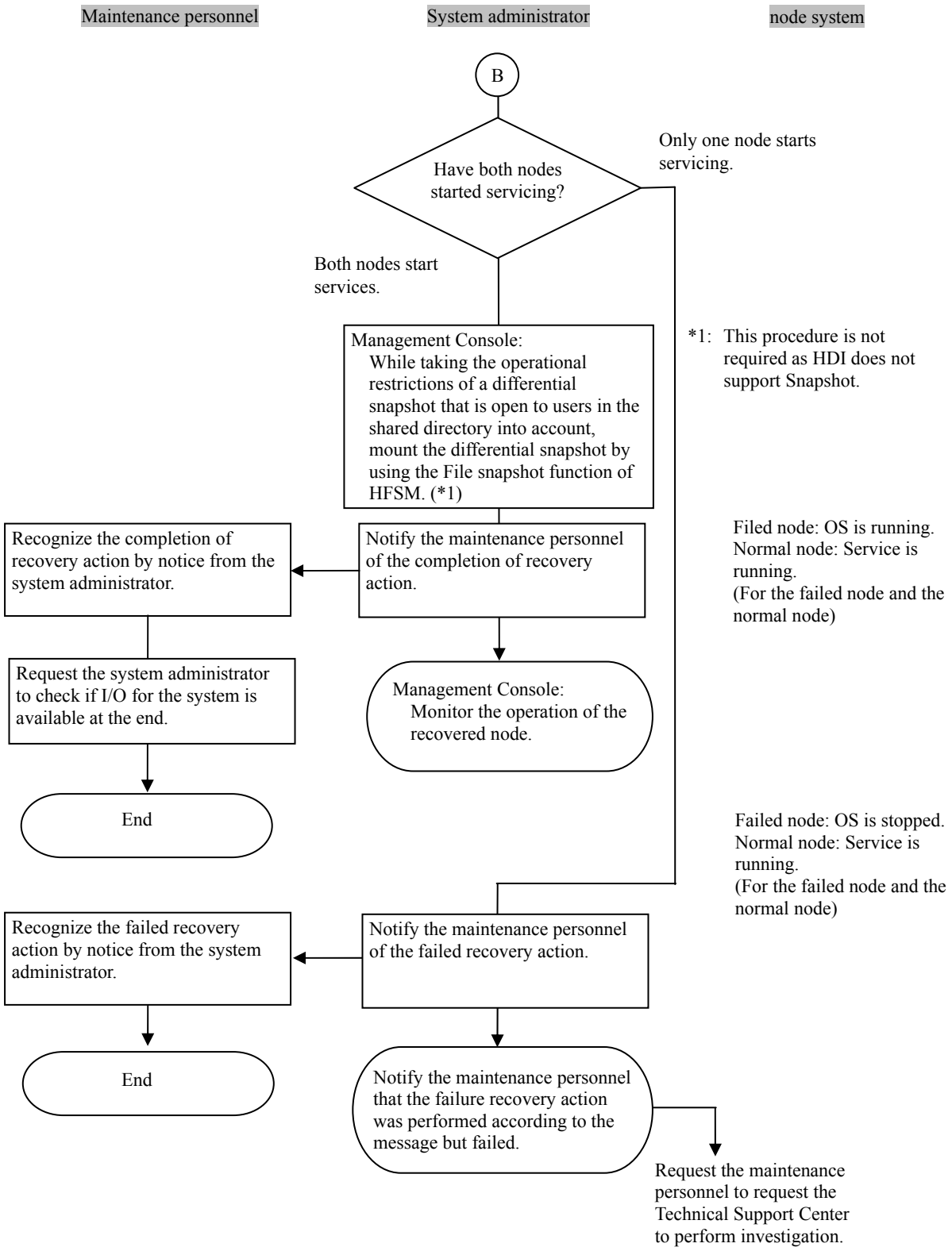


Figure 9.1.3.3.1-1 Procedure for KAQK39505-E Failure Recovery (3/3)

Copyright © 2014, Hitachi, Ltd.

9.1.3.3.2 Cluster management LU failure (when node service is started or stopped)

This section describes the recovery procedure for a cluster management LU failure (when node service is started or stopped) in the form of a flowchart. After this flow, perform the recovery as instructed by the Technical Support Center.

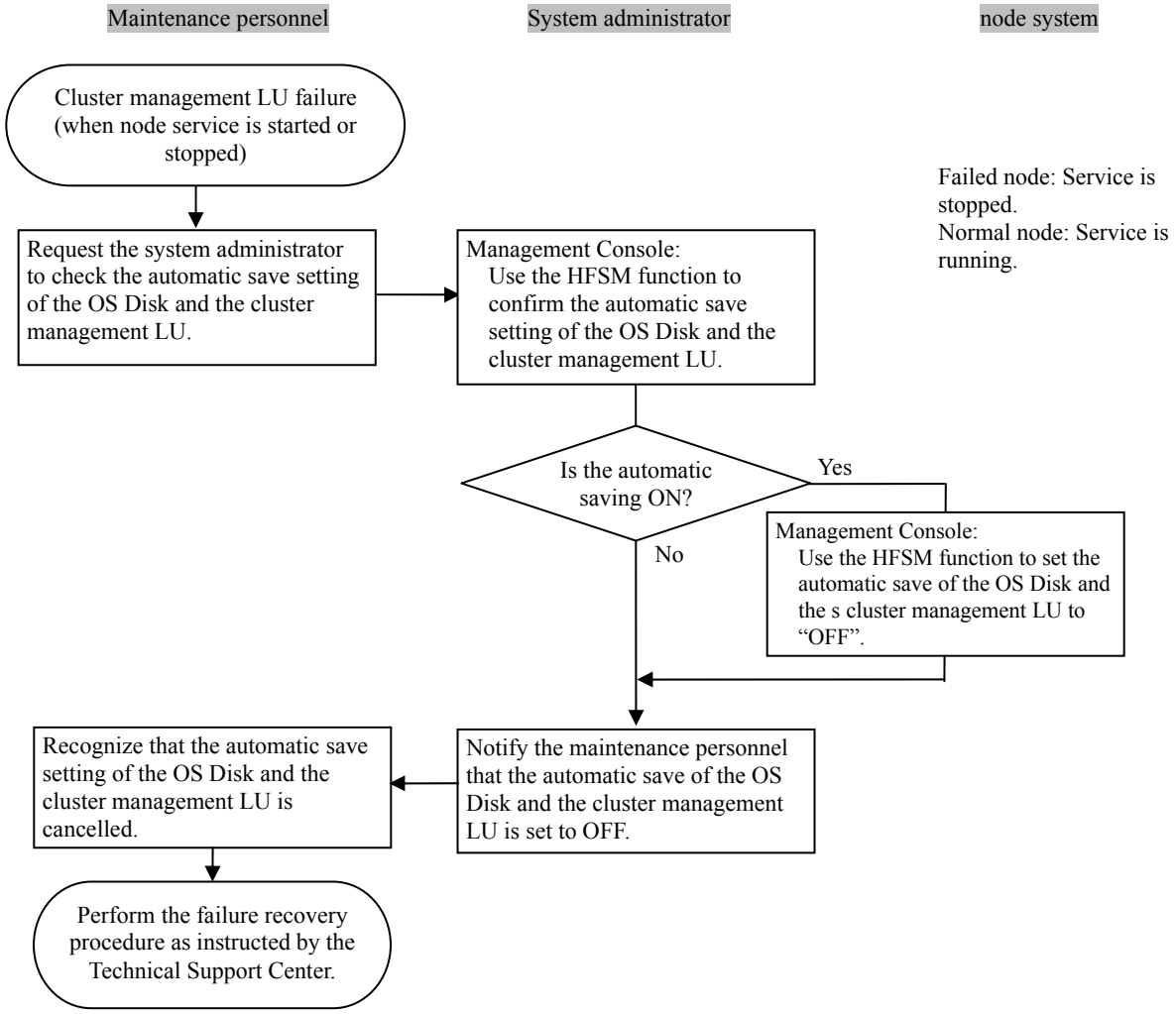
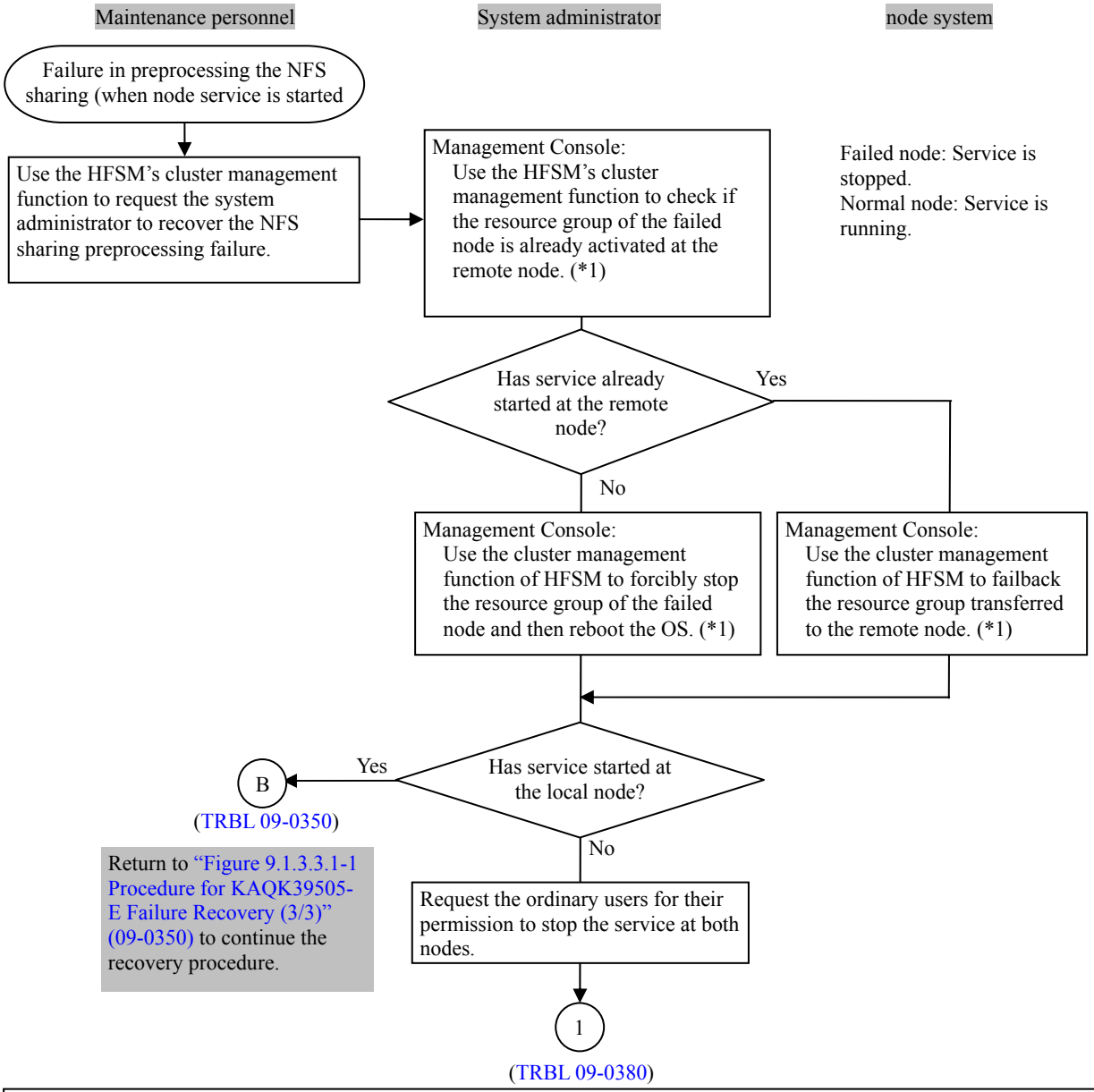


Figure 9.1.3.3.2-1 Recovery Procedure for a Cluster management LU Failure

Copyright © 2014, Hitachi, Ltd.

9.1.3.3.3 Failure in preprocessing the NFS sharing (when node service is started or stopped)

This section describes the recovery procedure for a failure which occurred during preprocessing of the NFS sharing (when node service is started or stopped) in the form of a flowchart.

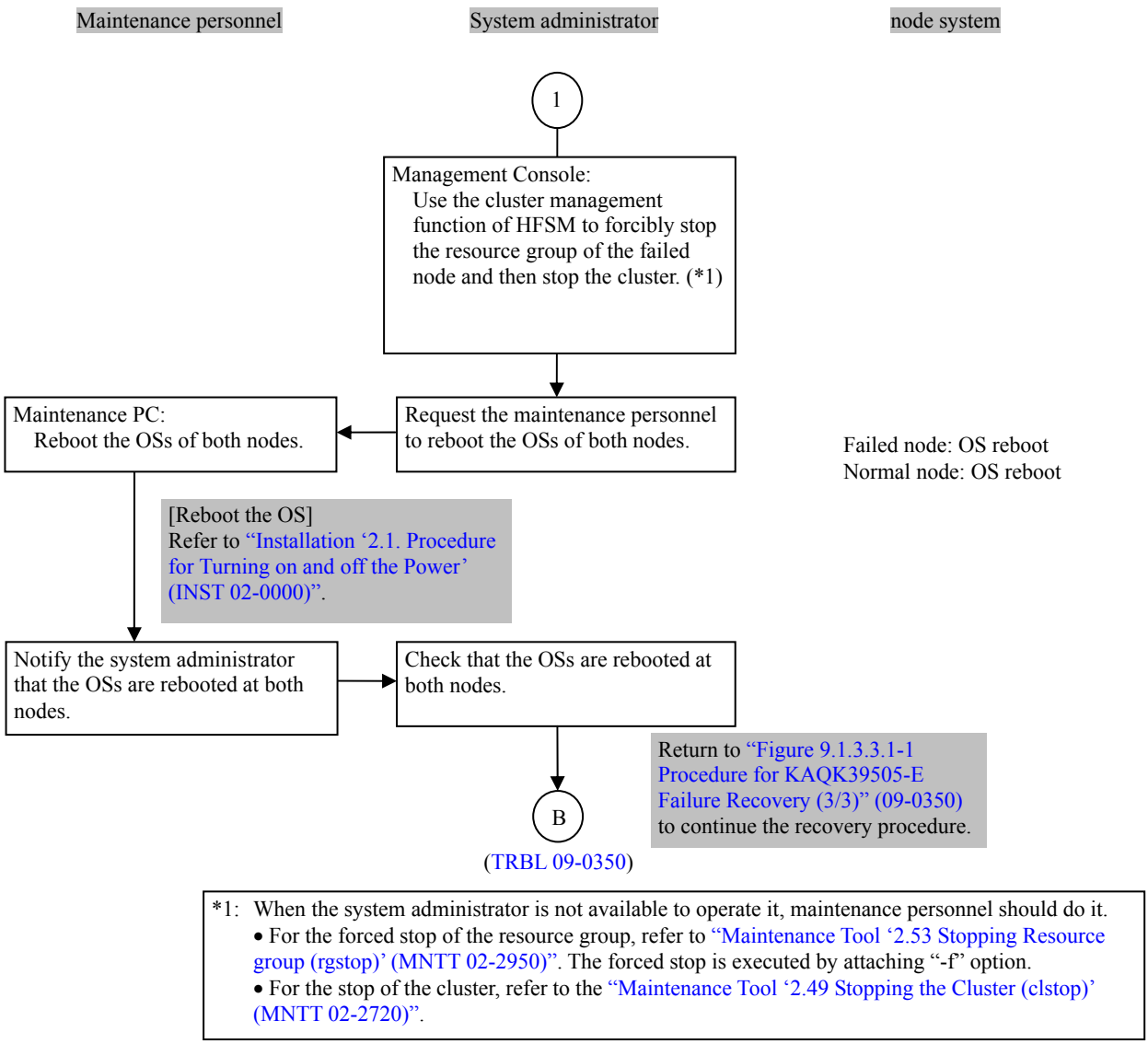


*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the confirmation of the cluster status, refer to "Maintenance Tool '2.2 Displaying the Cluster Status (clstatus)' (MNTT 02-0040)".
- For the failback of resource group, refer to "Maintenance Tool '2.54 Changing Resource group Execution node (rgmove)' (MNTT 02-3020)".
- For the forced stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)".

The forced stop is executed by attaching "-f" option.

Figure 9.1.3.3.3-1 Recovery Procedure for NFS Sharing Preprocessing Failure (1/2)

Copyright © 2014, Hitachi, Ltd.



*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the forced stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)". The forced stop is executed by attaching "-f" option.
- For the stop of the cluster, refer to the "Maintenance Tool '2.49 Stopping the Cluster (clstop)' (MNTT 02-2720)".

Figure 9.1.3.3.3-1 Recovery Procedure for NFS Sharing Preprocessing Failure (2/2)

Copyright © 2014, Hitachi, Ltd.

9.1.3.3.4 User LU failure (when node service is started or stopped)

This section describes the recovery procedure for a user LU failure (when node service is started or stopped) in the form of a flowchart.

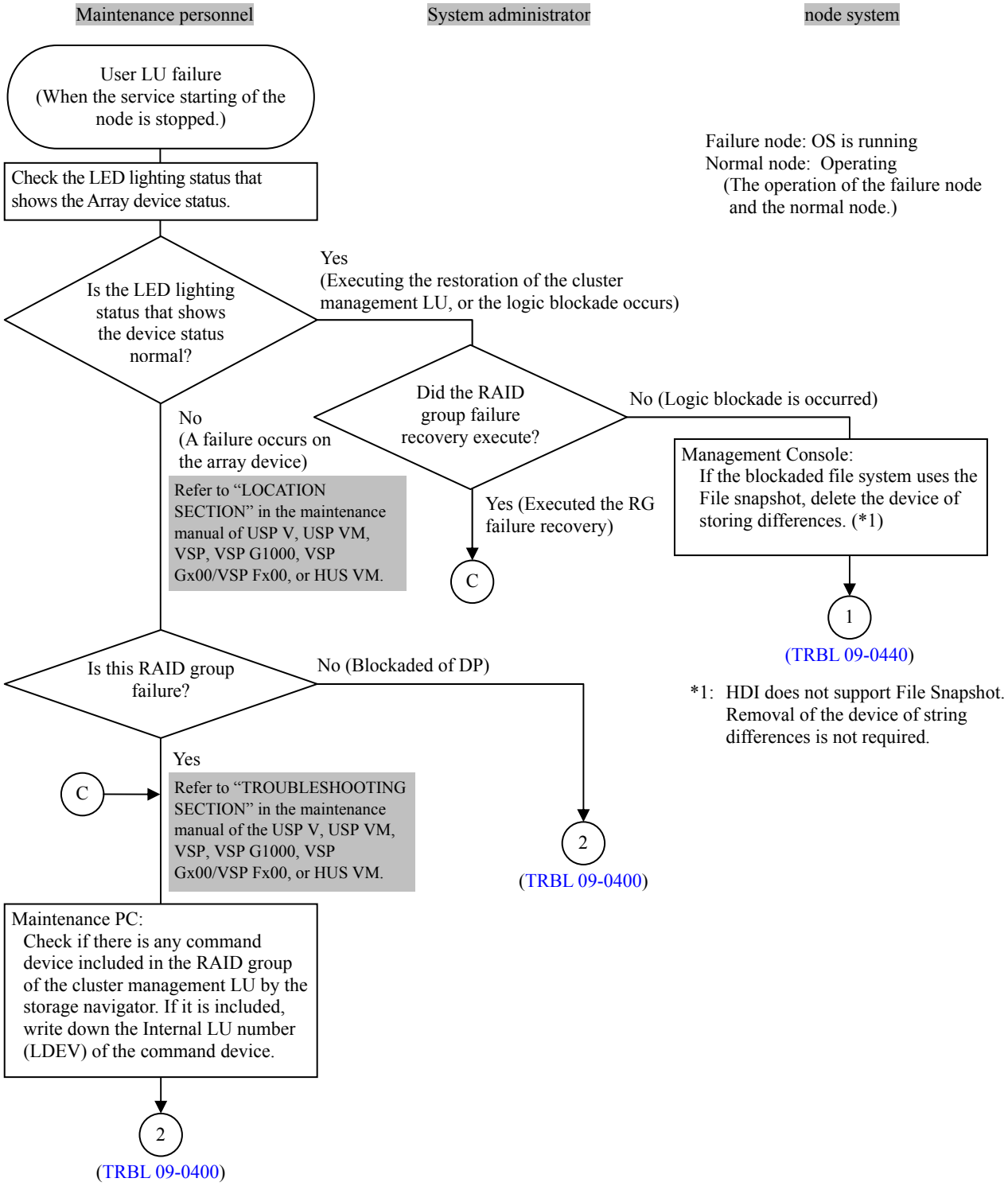
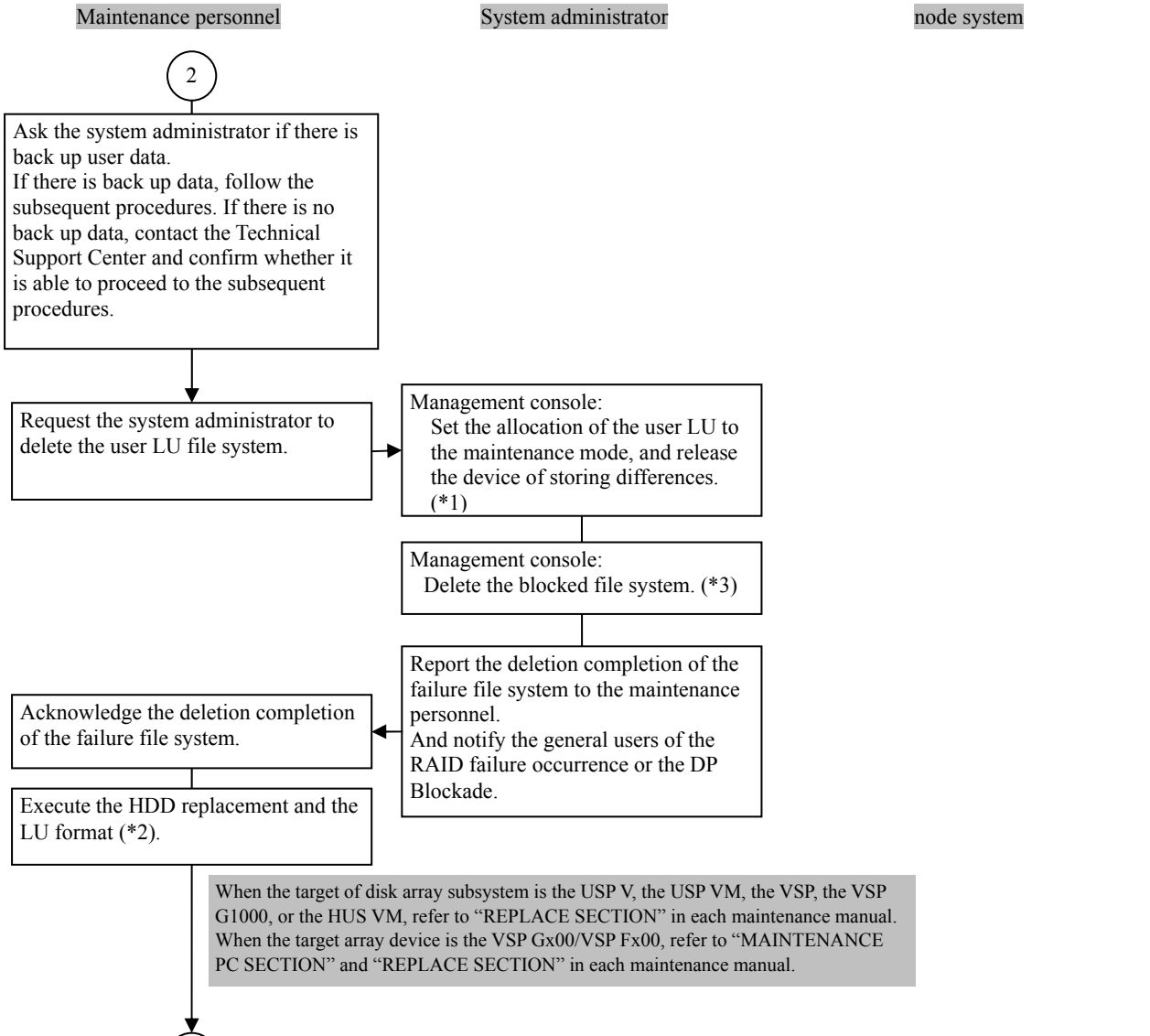


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (1/10)

Copyright © 2014, 2016, Hitachi, Ltd.



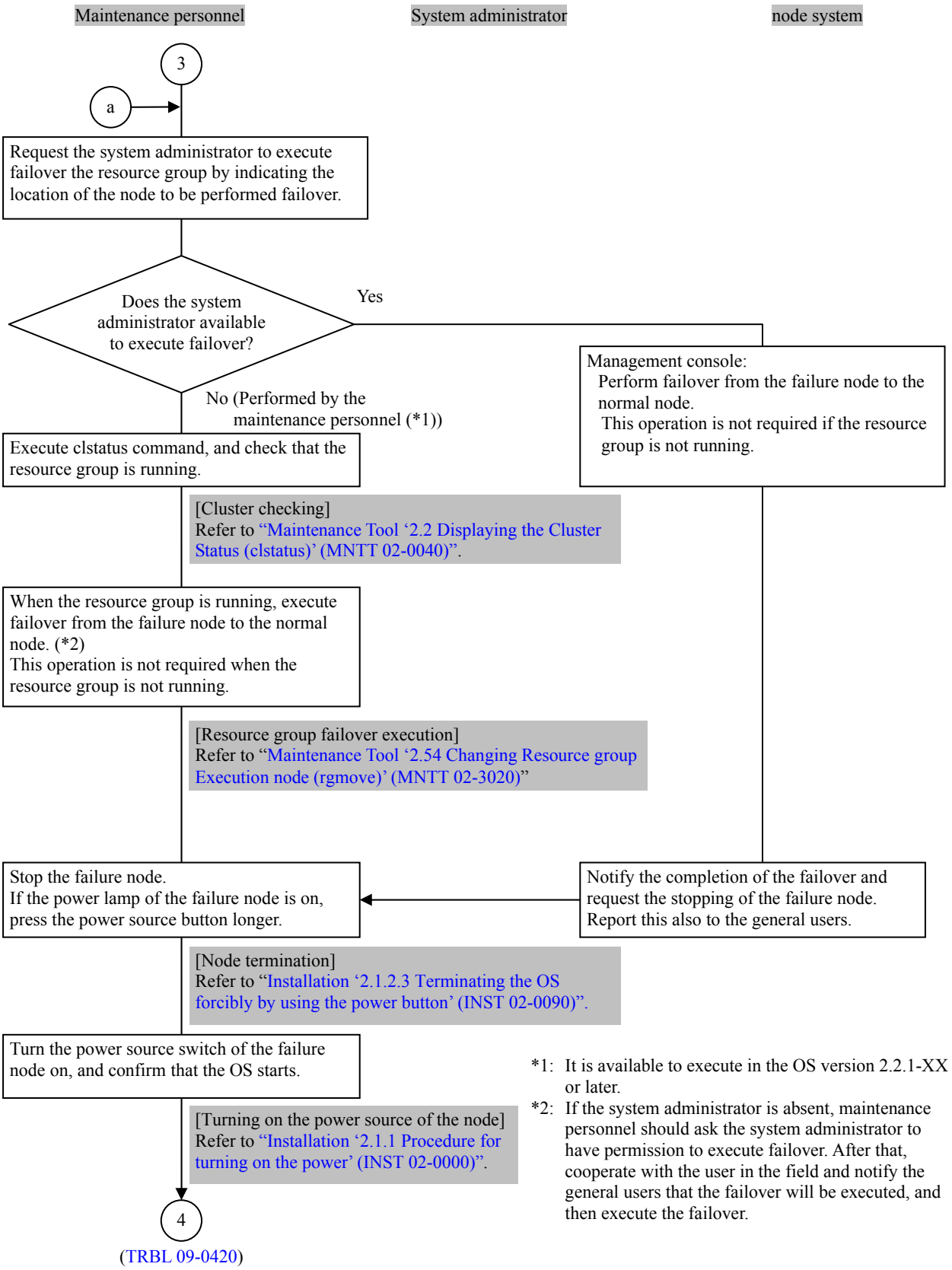
*1: HDI does not support Snapshot. Release of the device of string differences is not required.

*2: HDD replacement is not required if it is replaced already (when the cluster management LU is mixed.) Be careful not to format the cluster management LU.
Releasing S-VOL Disable is required if the LU format fails. Request the system administrator to use the RAID Manager and change it to the S-VOL Enable.
At the time of blocked DP, execute all the LU format in DP.

*3: At the time of blocked DP, delete all the file system in DP.

Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (2/10)

Copyright © 2014, 2016, Hitachi, Ltd.



*1: It is available to execute in the OS version 2.2.1-XX or later.

*2: If the system administrator is absent, maintenance personnel should ask the system administrator to have permission to execute failover. After that, cooperate with the user in the field and notify the general users that the failover will be executed, and then execute the failover.

Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (3/10)

Copyright © 2014, Hitachi, Ltd.

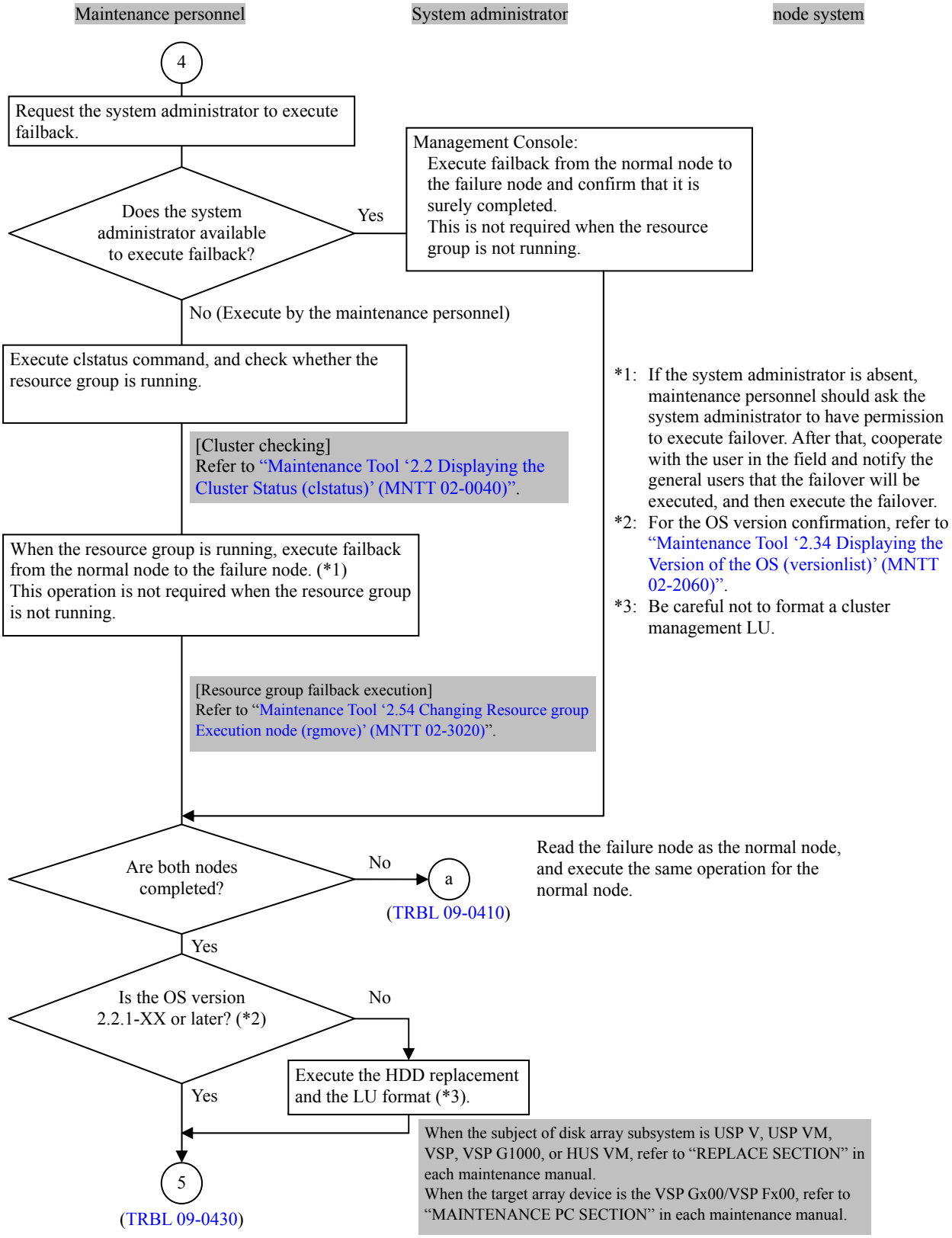


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (4/10)

Copyright © 2014, 2016, Hitachi, Ltd.

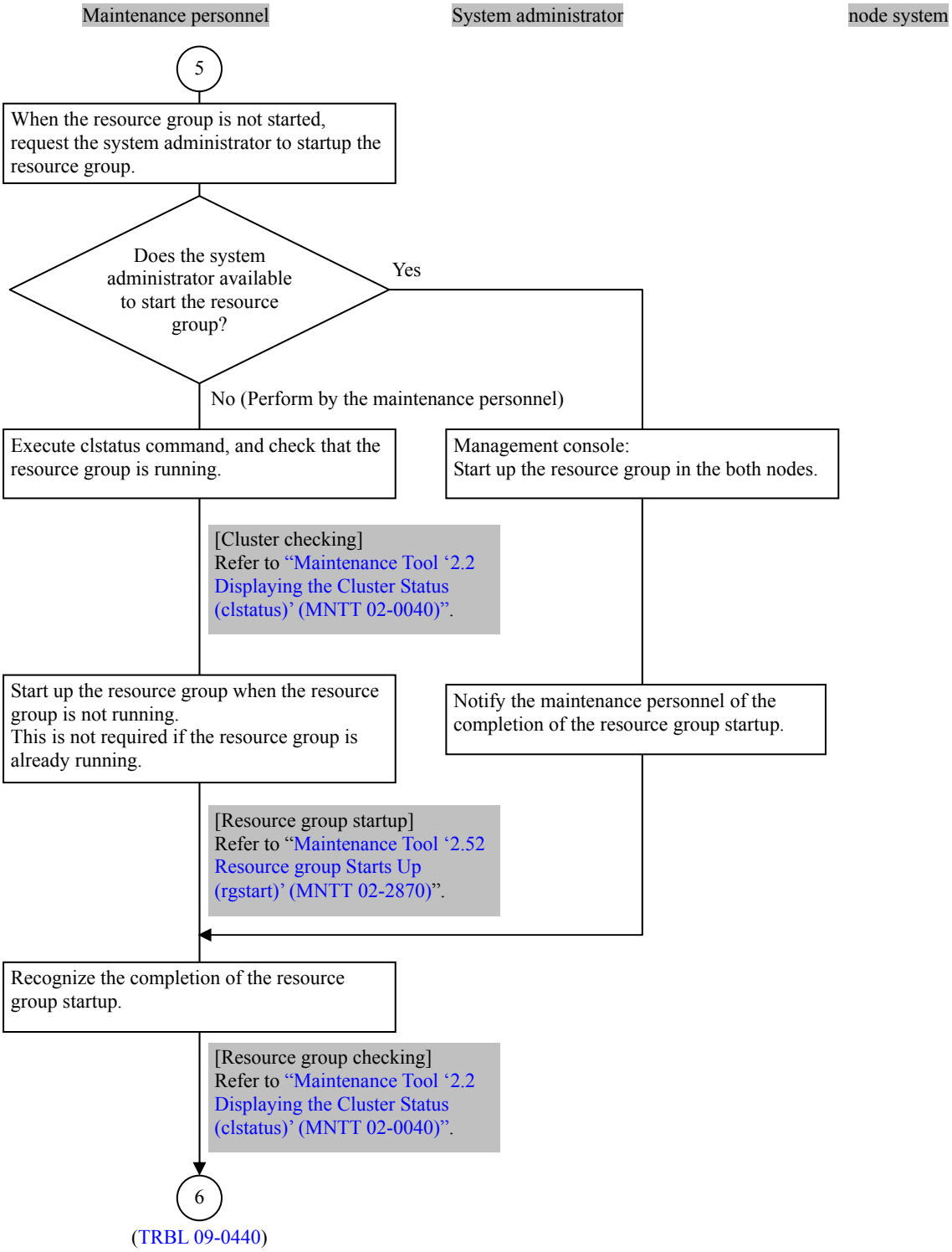
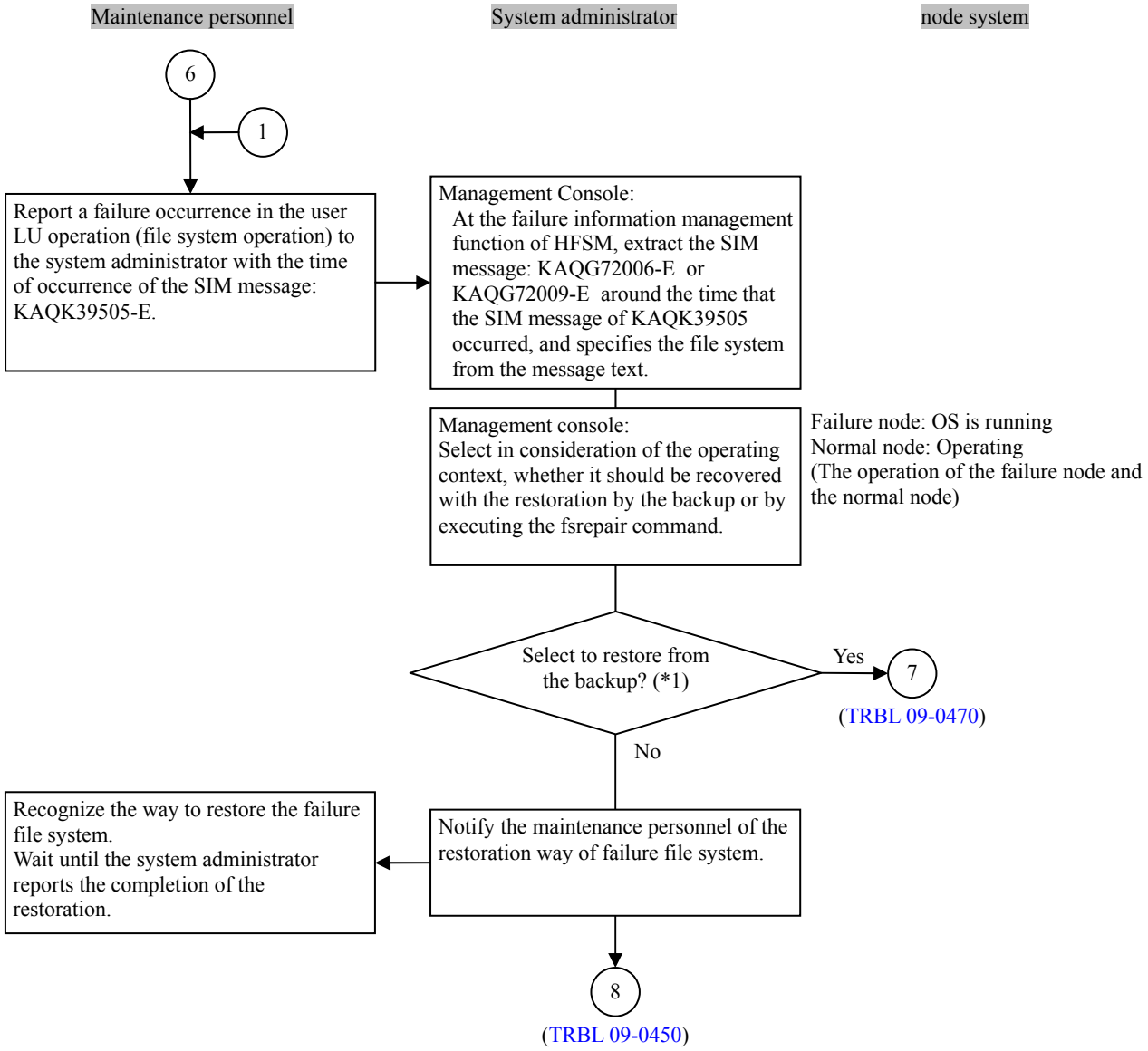


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (5/10)

Copyright © 2014, Hitachi, Ltd.



*1: Provide the following information to the system administrator, and follow his/her instruction.
- Recovery by executing restoration is to recreate the user file system and overwrite the backup data. Therefore, this method can only be recovered the file system status to the one that the date of backed up.
- Recovery by executing fsrepair command recovers the user file system before the occurrence of failures, by making match the file system integrity. However, destroyed data might not be recovered. It may take longer time for the recovery by the size of User LU and the number of files. Condition: 20,000,000 files in the state of no load. Time: (approx.) 2 hours.

NOTE:
- In the case of RAID failure, restoration from the backup can only be done.
- Execute the restoration from the backup in the case of the configuration of HDI for Cloud.

Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (6/10)

Copyright © 2014, Hitachi, Ltd.

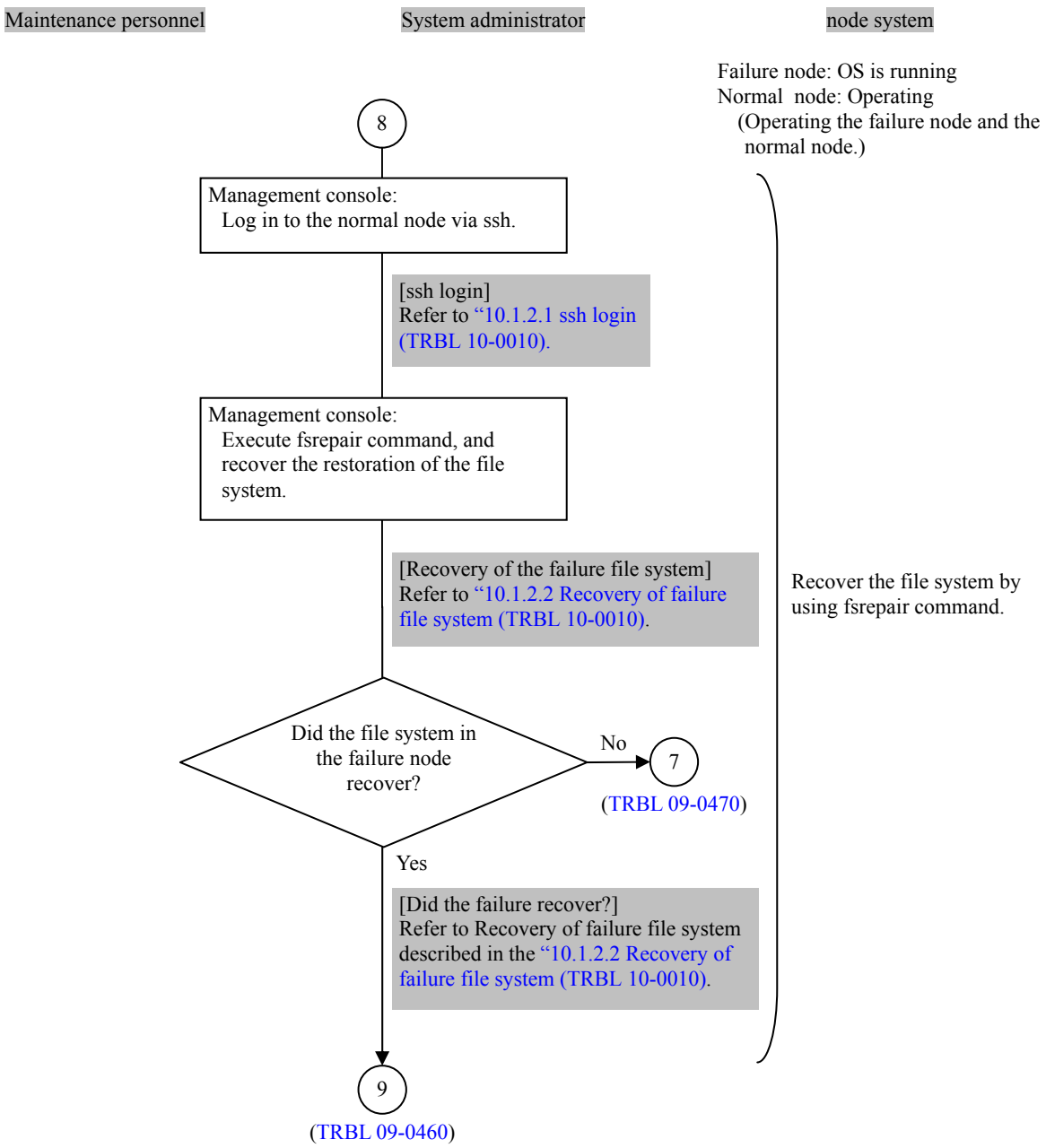


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (7/10)

Copyright © 2014, Hitachi, Ltd.

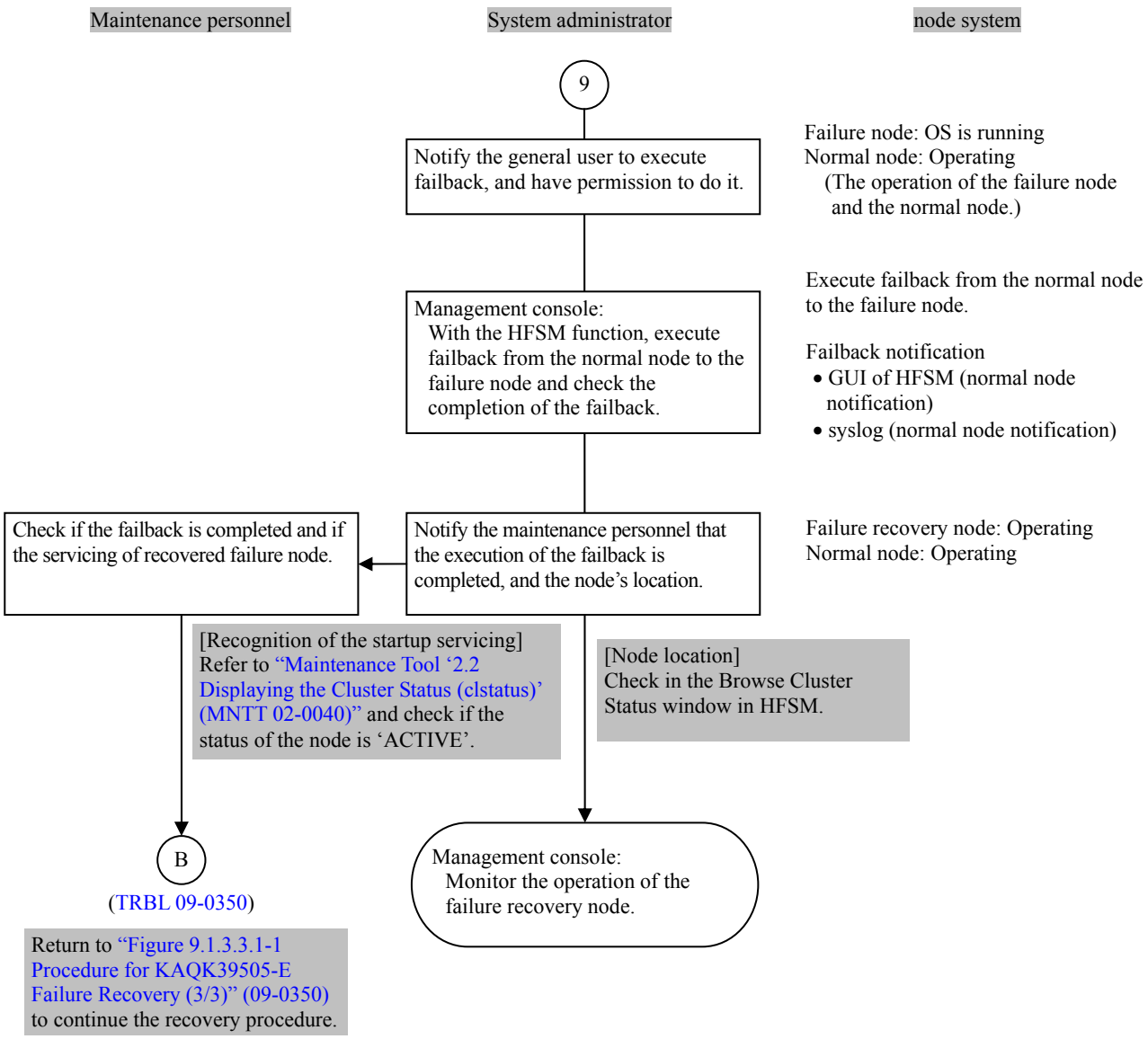
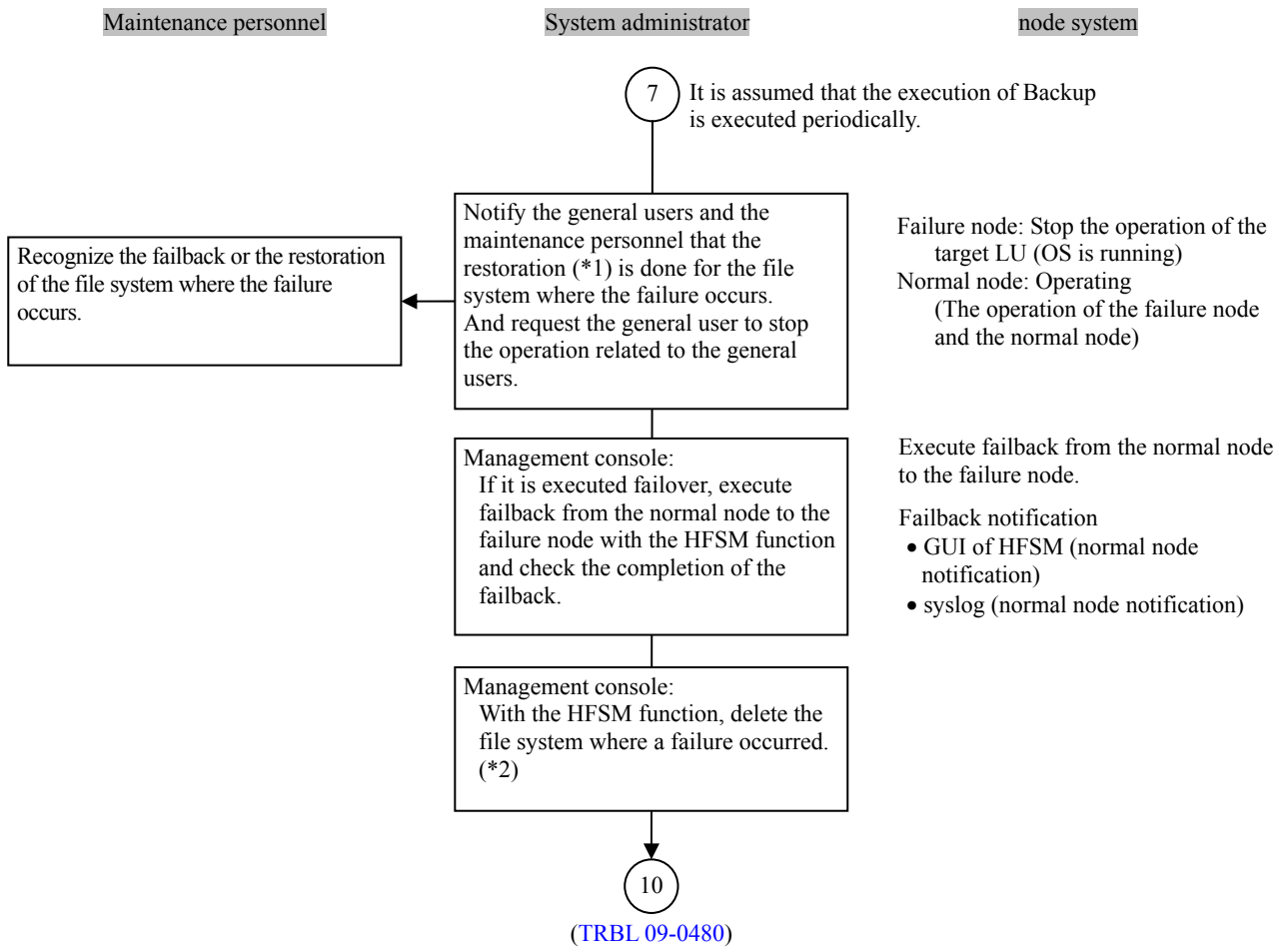


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (8/10)

Copyright © 2014, Hitachi, Ltd.



*1: If there are multiple file systems, execute the restoration process also for the other file systems.
*2: If the file system of the failure LU uses the File snapshot, release the device of storing differences before deleting the file system.

Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (9/10)

Copyright © 2014, Hitachi, Ltd.

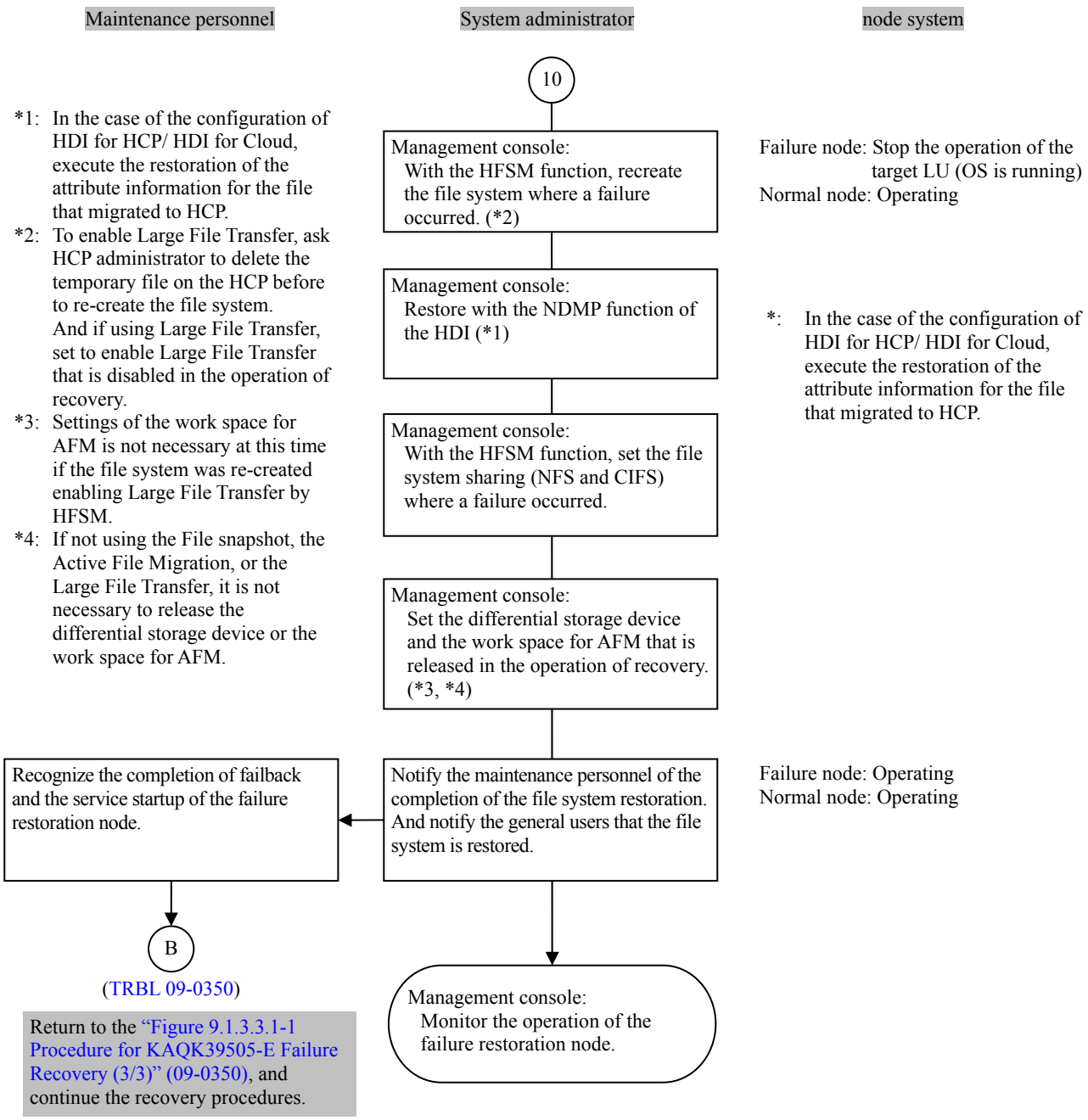
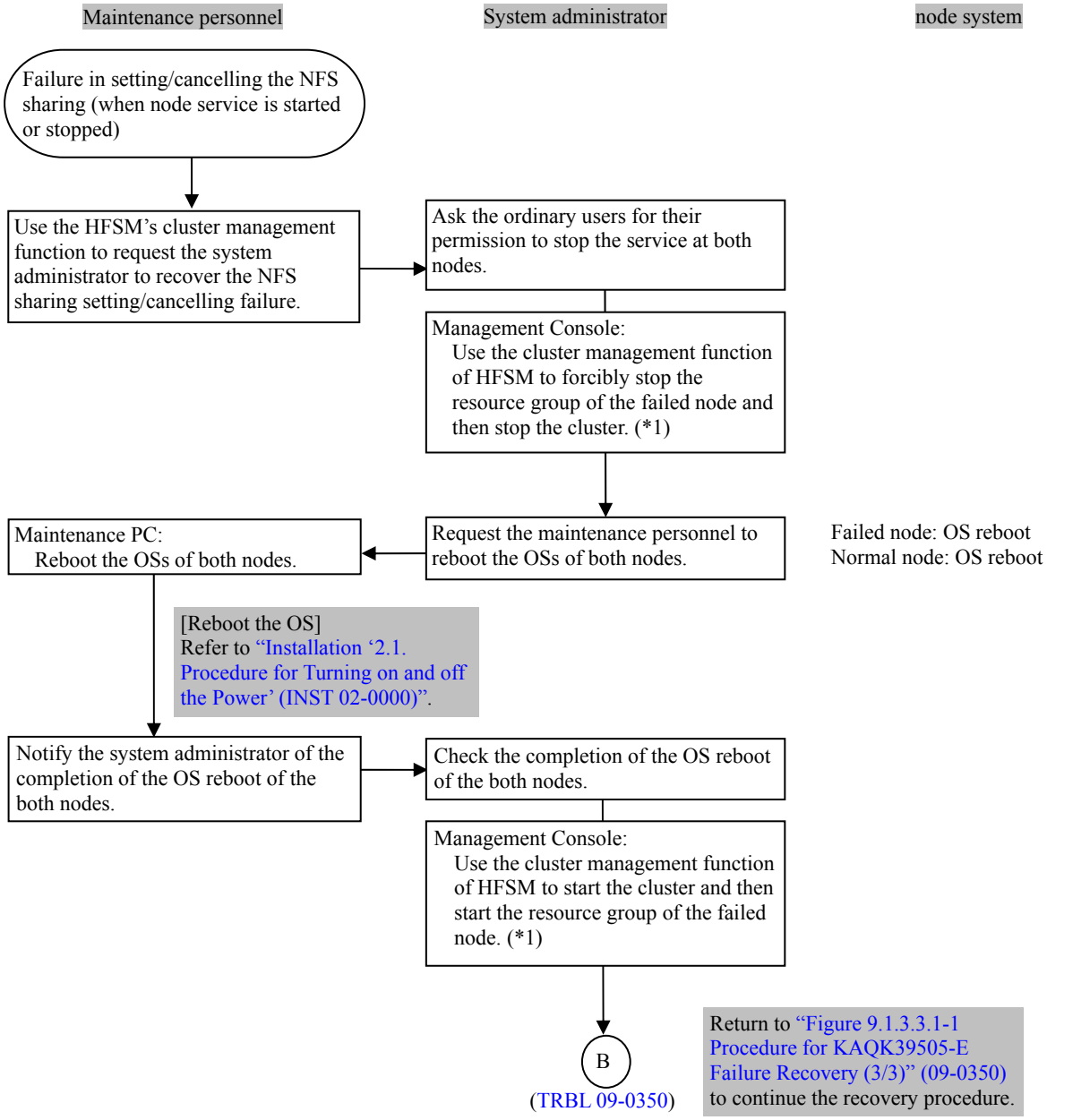


Figure 9.1.3.3.4-1 Recovery Procedure for User LU Failure (10/10)

Copyright © 2014, 2017, Hitachi, Ltd.

9.1.3.3.5 Failure in setting/cancelling the NFS sharing (when node service is started or stopped)

This section describes the recovery procedure for a user LU failure (when node service is started or stopped) in the form of a flowchart.



*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the forced stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)". The forced stop is executed by attaching "-f" option.
- For the stop of the cluster, refer to the "Maintenance Tool '2.49 Stopping the Cluster (clstop)' (MNTT 02-2720)".
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".

Figure 9.1.3.3.5-1 Recovery Procedure for NFS Sharing Setting/Cancelling Failure

Copyright © 2014, 2015, Hitachi, Ltd.

9.1.3.3.6 Up/down failure of the virtual IP (when node service is started or stopped)

This section describes the recovery procedure for a virtual IP up/down failure (when node service is started or stopped) in the form of a flowchart.

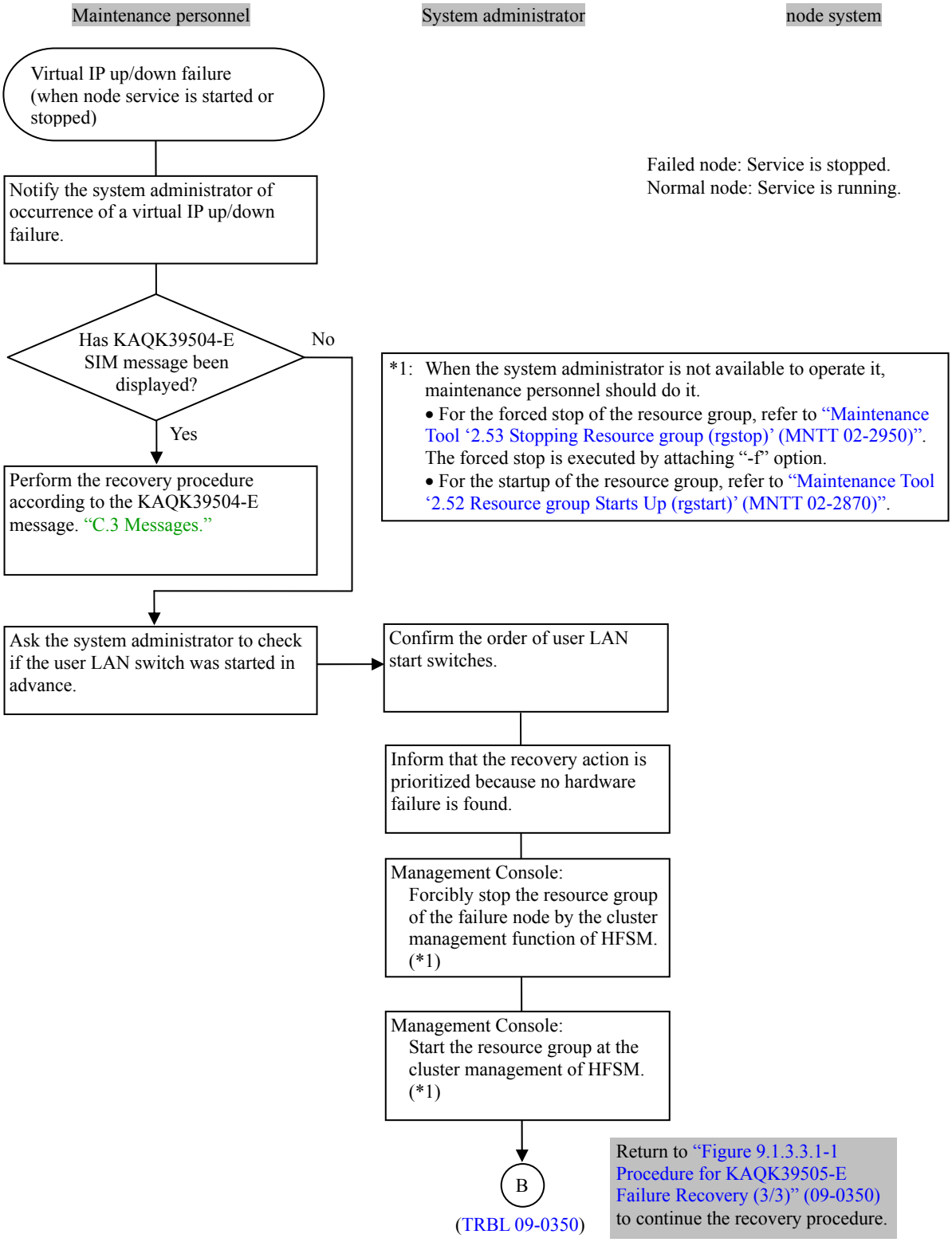
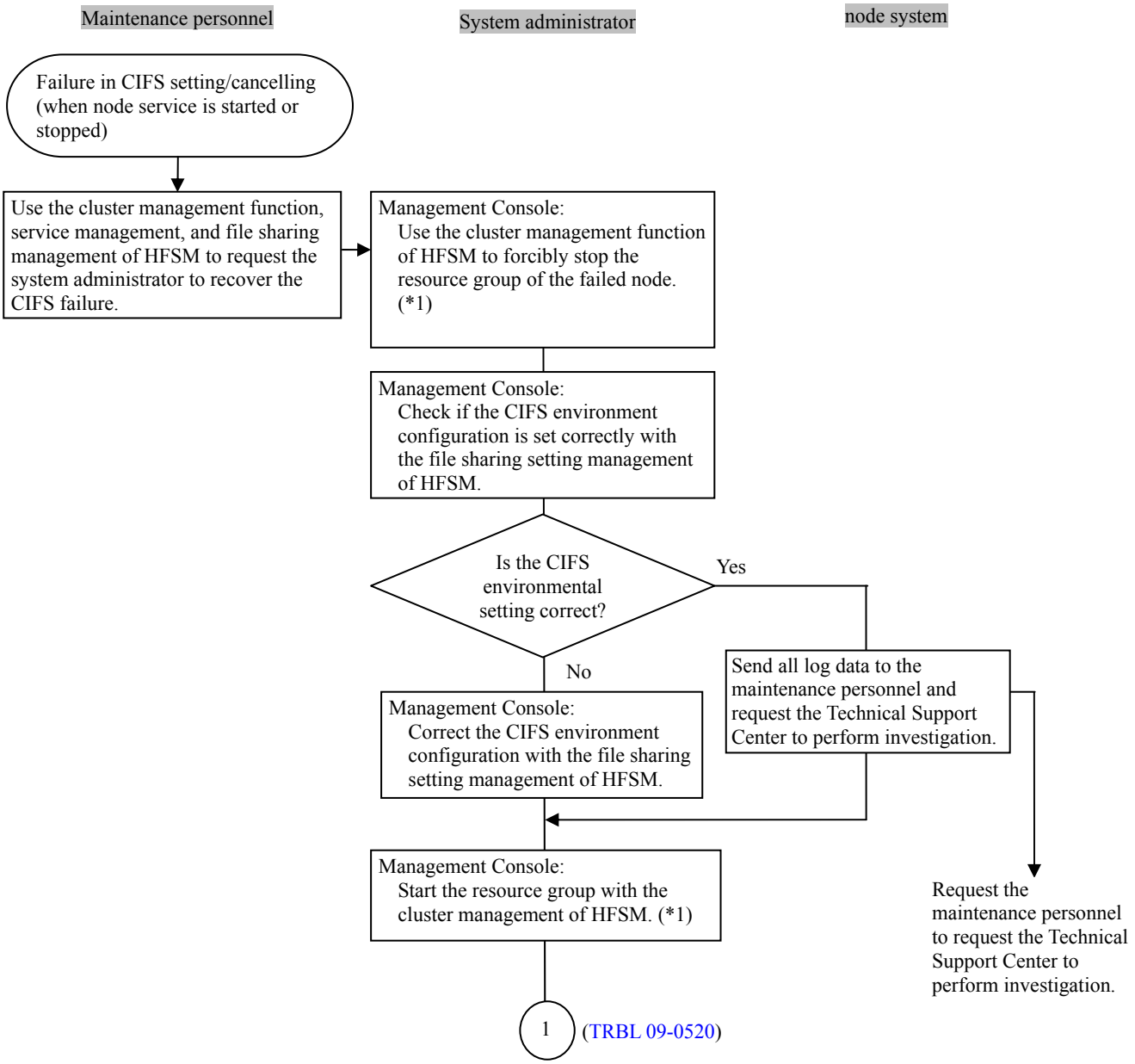


Figure 9.1.3.3.6-1 Recovery Procedure for Virtual IP Up/Down Failure

Copyright © 2014, Hitachi, Ltd.

9.1.3.3.7 Failure in CIFS setting/cancelling (when node service is started or stopped)

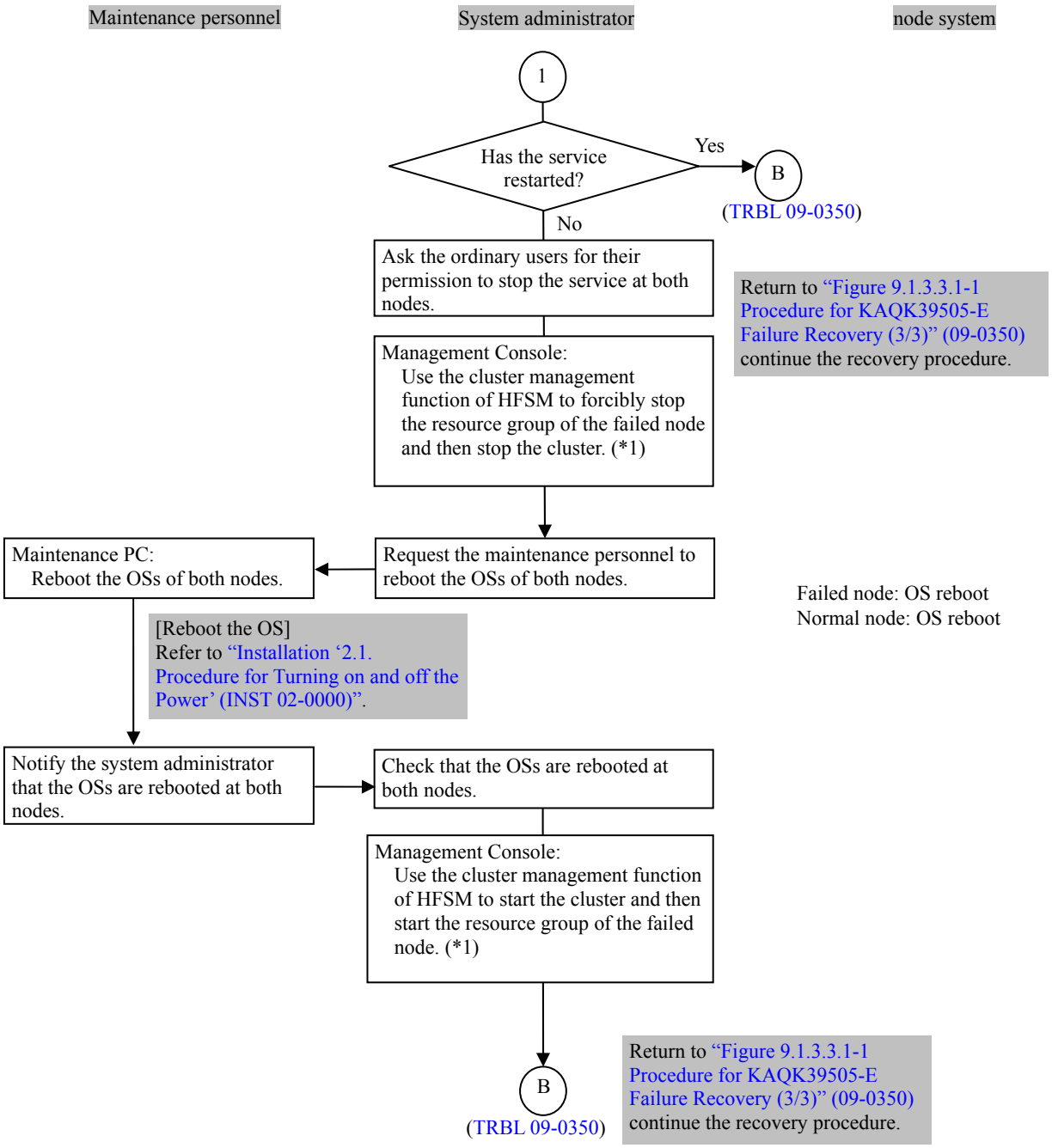
This section describes the recovery procedure for the CIFS setting/cancelling failure (when node service is started or stopped) in the form of a flowchart.



*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the forced stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)". The forced stop is executed by attaching "-f" option.
- For the stop of the cluster, refer to the "Maintenance Tool '2.49 Stopping the Cluster (clstop)' (MNTT 02-2720)".
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".

Figure 9.1.3.3.7-1 Recovery Procedure for CIFS Setting/Cancelling Failure (1/2)

Copyright © 2014, Hitachi, Ltd.



*1: When the system administrator is not available to operate it, maintenance personnel should do it.
- For the forced stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)". The forced stop is executed by attaching "-f" option.
- For the stop of the cluster, refer to the "Maintenance Tool '2.49 Stopping the Cluster (clstop)' (MNTT 02-2720)".
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".

Figure 9.1.3.3.7-1 Recovery Procedure for CIFS Setting/Cancelling Failure (2/2)

Copyright © 2014, Hitachi, Ltd.

9.1.3.3.8 File snapshot or File Version Restore function failure (when node service is started or stopped)

This section describes the recovery procedure for the File snapshot or file version restore function failure (when node service is started or stopped) in the form of a flowchart.

NOTE: HDI does not support the Snapshot function.

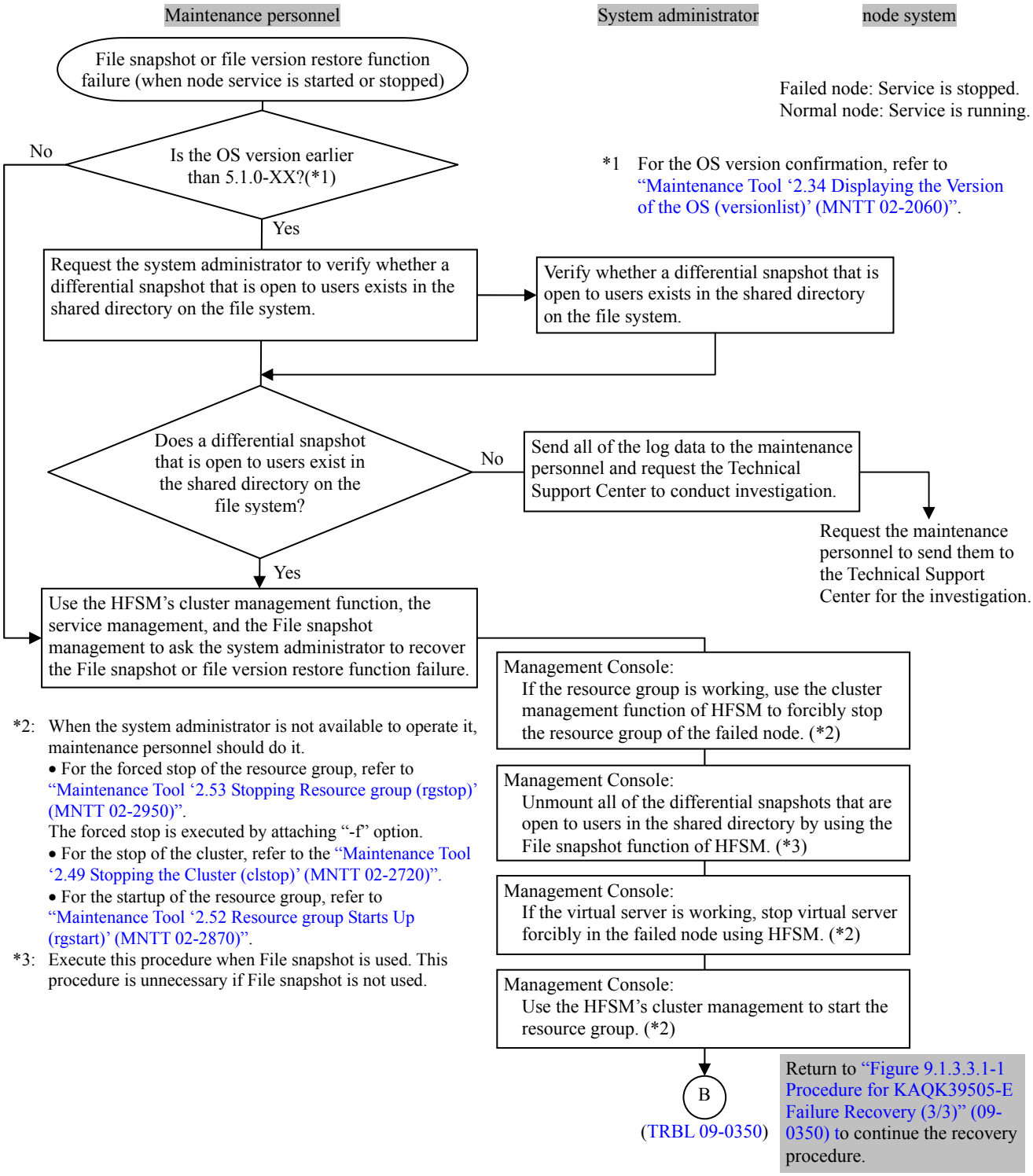


Figure 9.1.3.3.8-1 Recovery Procedure for a File snapshot or File Version Restore Function Failure

Copyright © 2014, 2016, Hitachi, Ltd.

9.1.3.4 Recovery from KAQK39602-E failure

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.1 Procedure for KAQK39602-E failure recovery

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.2 File system failure

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.3 Failure in starting/ stopping the NFS sharing

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.4 Up/down failure of the virtual IP

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.5 Failure in CIFS setting/canceling

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

9.1.3.4.6 File snapshot or File Version Restore Function Failure

KAQK39602-E is the failure message which is output when a failure occurs on Virtual Server.

HDI does not support Virtual Server.

Copyright © 2014, Hitachi, Ltd.

9.1.4 Upgrading the Software by Updating the OS Version

As the final recovery procedure for KAQK39500-E or KAQK39505-E, update the OS version to upgrade the software.

This section describes the procedure to upgrade the software by updating the OS version.

NOTE: Before performing failback from the normal node to the failed node, request the system administrator to check that the data LAN of the failed node is in the link-up state.

Table 9.1.4-1 provides the overview of the software upgrading by updating the OS version.

Table 9.1.4-1 Procedure of Software Upgrading by Updating the OS Version

Procedure	Process	Remarks
1	Obtain the update version (OS).	—
2	Start the OS.	Execute this step when the OS is stopped.
3	Stop the node.	—
4	Update the OS to upgrade the software.	—
5	Start the node.	—
6	Return the automatic save setting of the OS LU and the cluster management LU to the setting before the failure occurrence.	—
7	Perform failback.	—

NOTE:
- For software upgrading, the node in a cluster must be of the same version. Therefore, upgrading is performed on a cluster basis.
- When the processing on node0 is completed and the processing is to be applied to node1, request the system administrator for failback and failover from node1 to node0. After the process to upgrade the OS for node1, request the system administrator for failover of the node0.
- Due to software upgrading, failover is performed two times. This may affect client's I/O operation. Request the system administrator to check if the administrator recognizes this.
- Be sure to get the backup data before the updating installation. When the OS version is 3.0.0-XX or later, the maintenance personnel should execute the updating installation. When the OS version is earlier than 3.0.0-XX, request the system administrator to get the backup data and execute the updating operation after confirming that the data is backed up.

The flowchart shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status. Upgrading procedures for the maintenance personnel and the system administrator are shown respectively.

Copyright © 2014, Hitachi, Ltd.

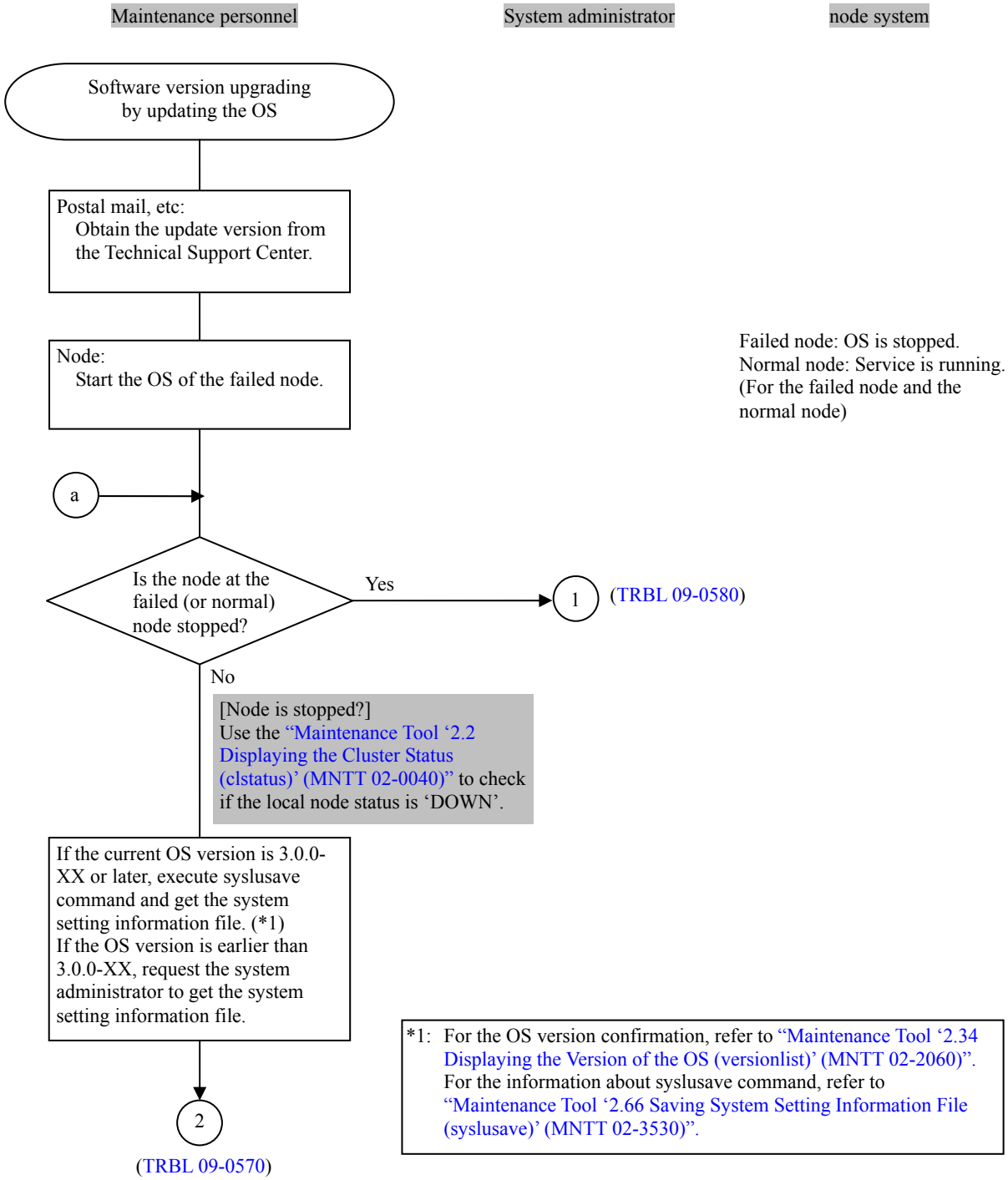
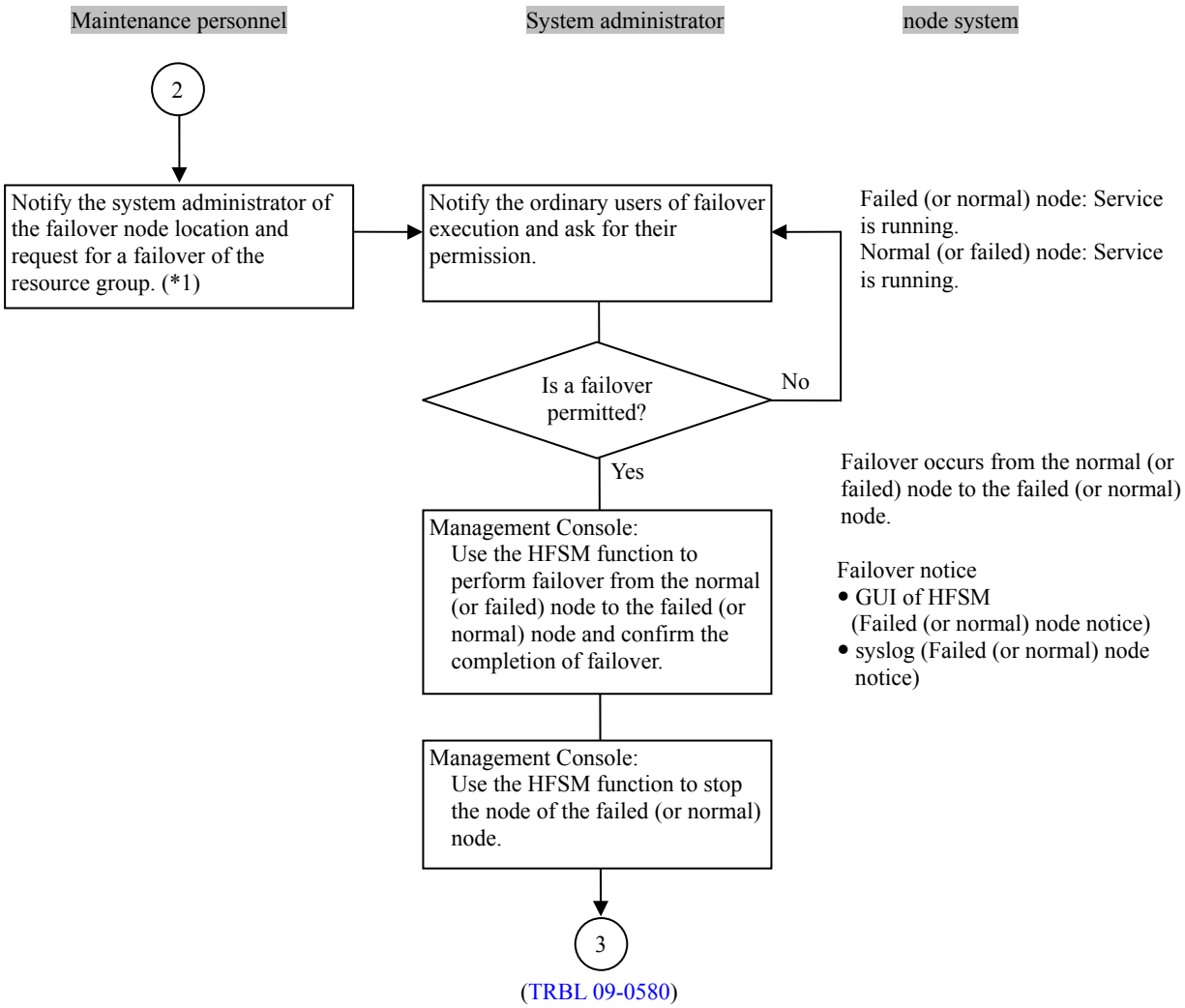


Figure 9.1.4-1 Upgrading the Software by Updating the OS Version (1/4)

Copyright © 2014, Hitachi, Ltd.



*1: When the system administrator is not available to operate it, maintenance personnel should do it. For the execution procedure, refer to "Maintenance Tool '3.1 Failover and Node Termination to Execute the OS stop or the OS reboot' (MNTT 03-0000)".

Figure 9.1.4-1 Upgrading the Software by Updating the OS Version (2/4)

Copyright © 2014, Hitachi, Ltd.

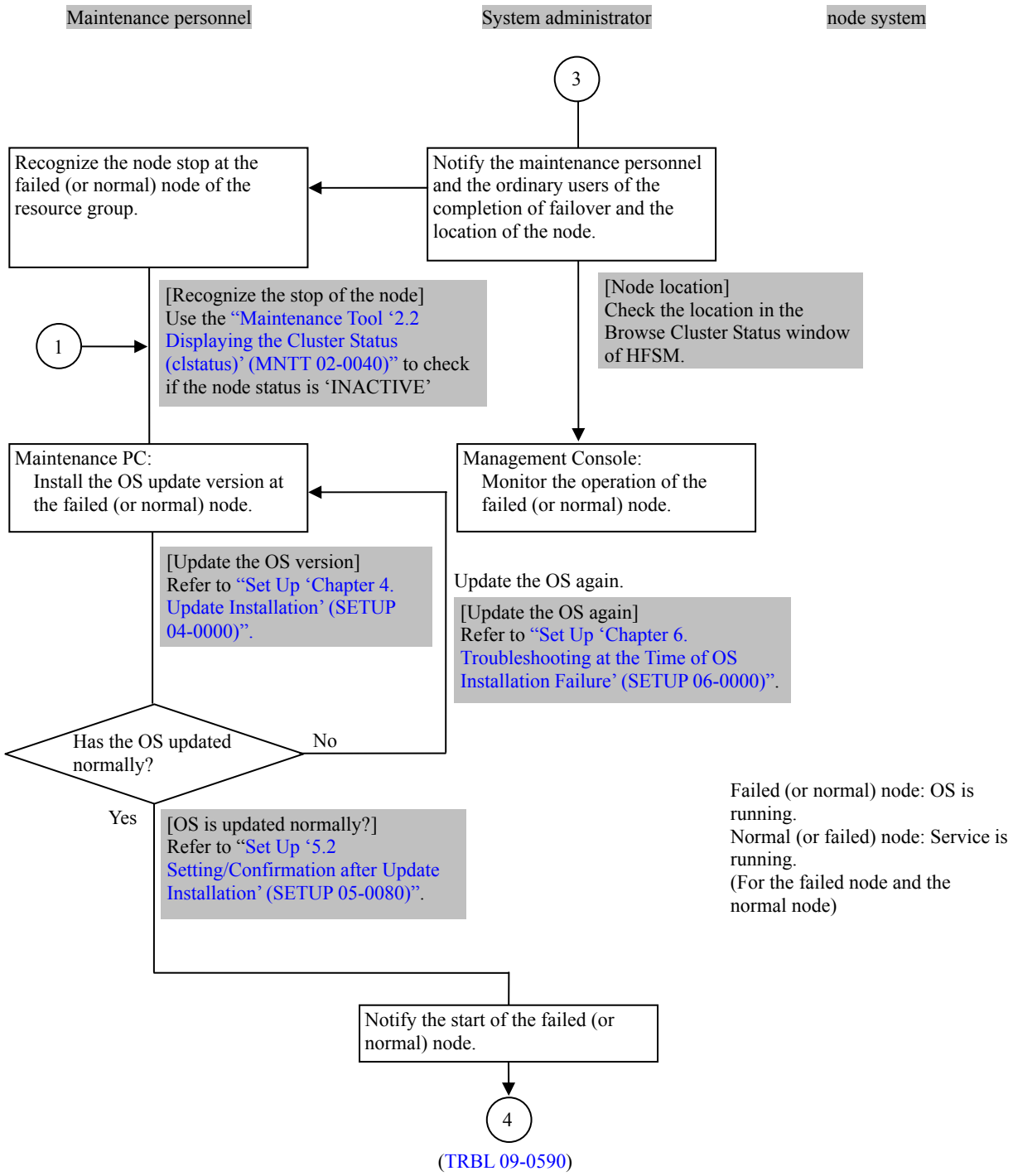


Figure 9.1.4-1 Upgrading the Software by Updating the OS Version (3/4)

Copyright © 2014, Hitachi, Ltd.

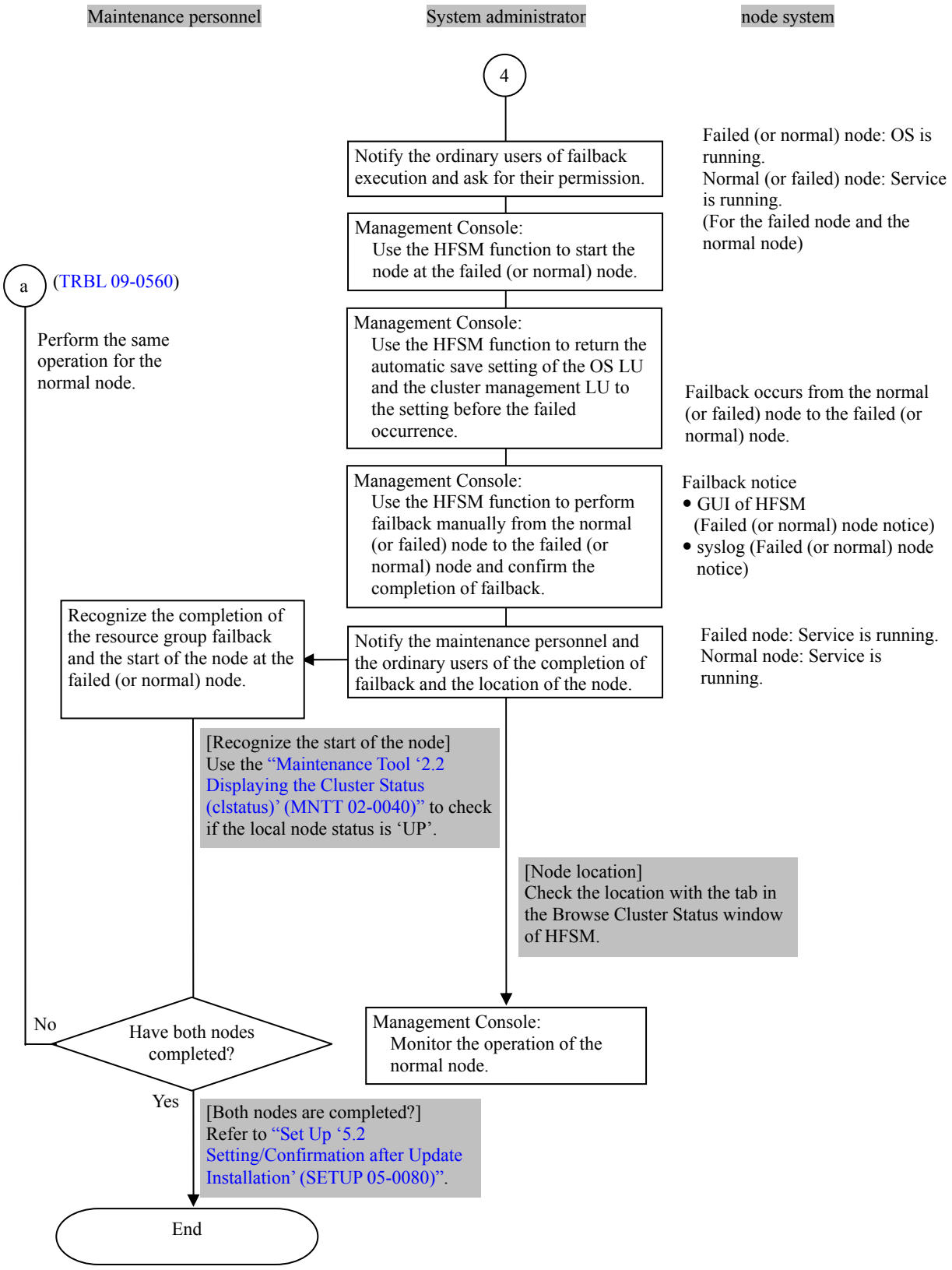


Figure 9.1.4-1 Upgrading the Software by Updating the OS Version (4/4)

Copyright © 2014, Hitachi, Ltd.

9.1.5 Software Recovery by Installing the OS Initially

As the failure recovery procedure for KAQK39500-E Detail=00 02 00 02, execute the initial OS installation.

This section describes the procedure to execute initial OS installation.

Table 9.1.5-1 provides the overview of the re-installation of the software by the initial OS installation.

Table 9.1.5-1 Procedure of Initial OS Installation

Procedure	Process	Remarks
1	Stop the node.	—
2	Execute the initial OS installation.	—
3	Start the node.	—
4	Execute the OS DISK recovery.	Reboot the system.
5	Return the automatic save setting of the OS LU and the cluster management LU to the setting before the failure occurrence.	—
6	Perform failback.	—

The flowchart shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status. Initial installation procedure of OS for the maintenance personnel and the system administrator are shown respectively.

Copyright © 2014, Hitachi, Ltd.

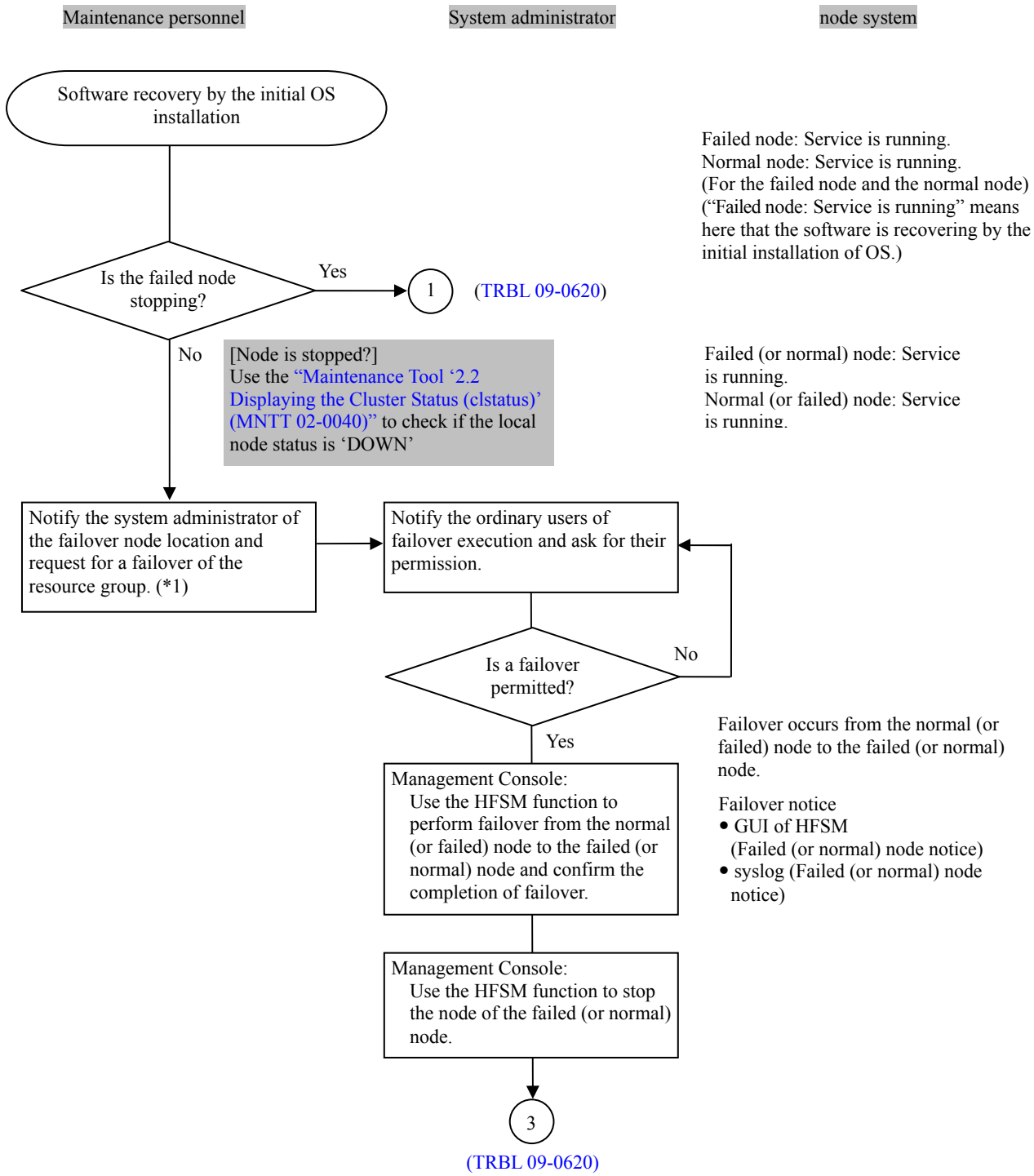


Figure 9.1.5-1 Recovery of the software by the initial OS installation (1/3)

Copyright © 2014, Hitachi, Ltd.

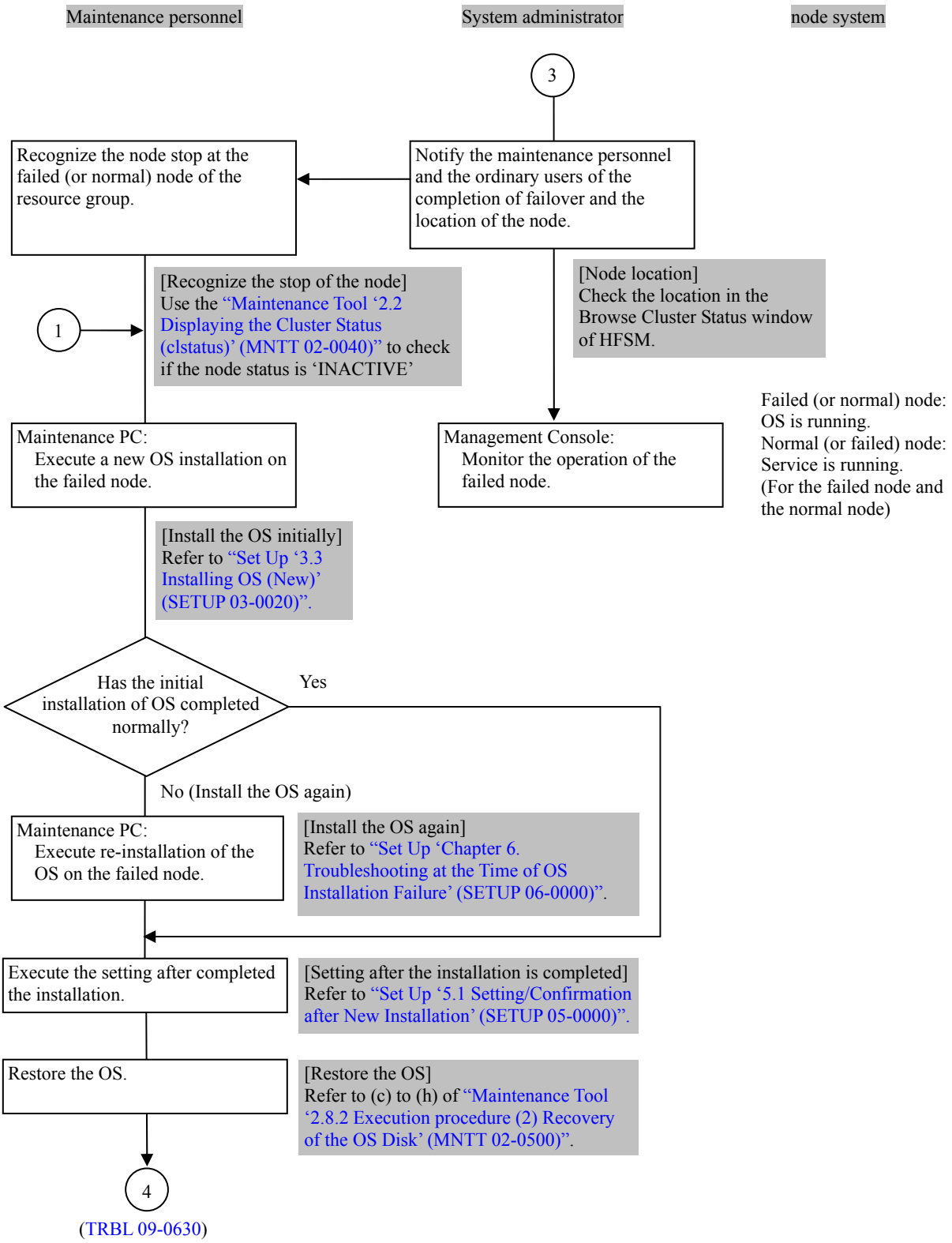


Figure 9.1.5-1 Recovery of the software by the initial OS installation (2/3)

Copyright © 2014, Hitachi, Ltd.

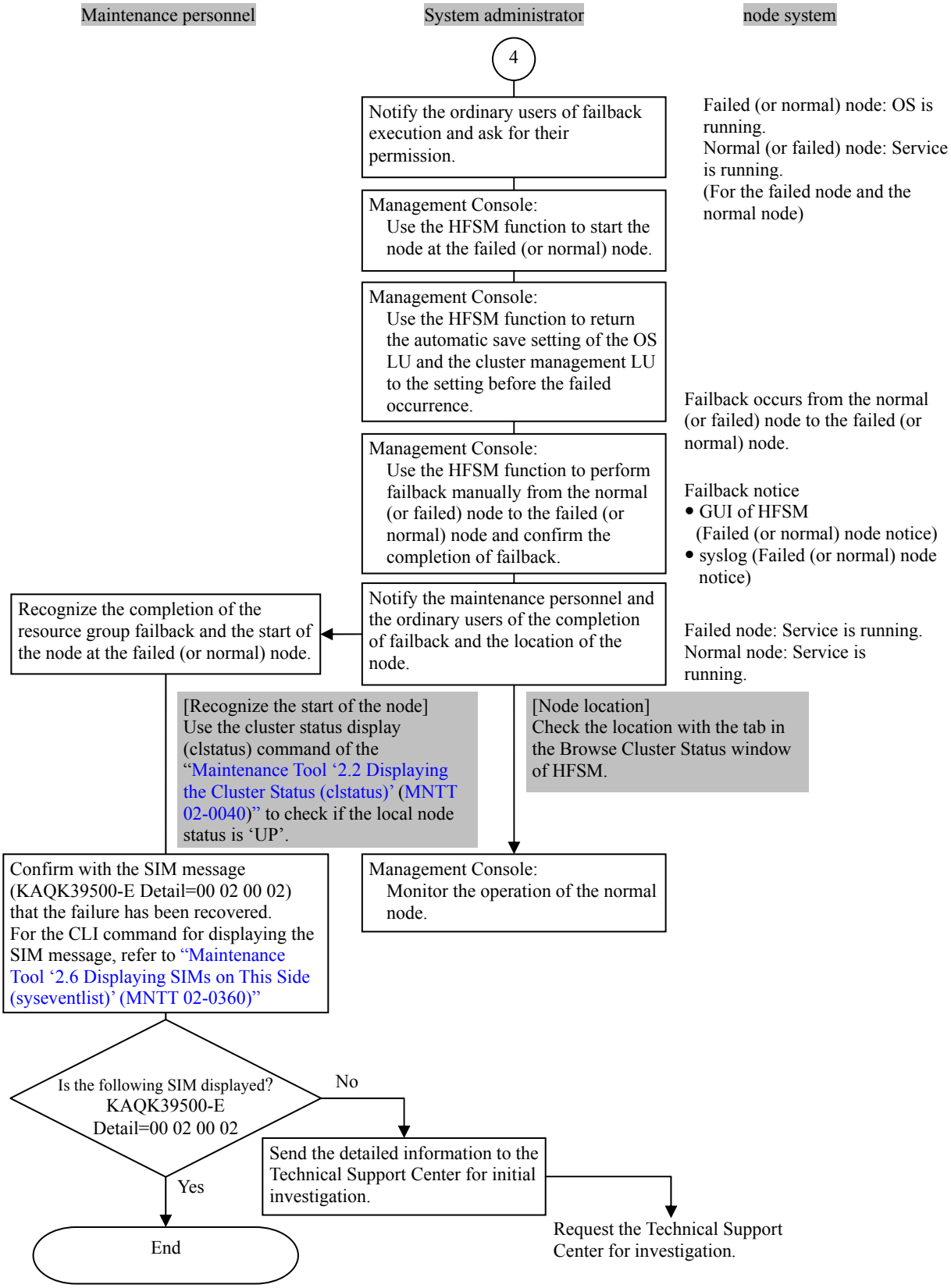


Figure 9.1.5-1 Recovery of the software by the initial OS installation (3/3)

Copyright © 2014, Hitachi, Ltd.

9.2 Confirmation of Hardware Failure Recovery and Recovery Procedure for Software Failure at the Single Node Configuration

9.2.1 Overview of Confirmation of the Entire Node after Hardware Failure Recovery and Recovery Procedure for Software Failure

The overview of confirmation of the entire node after recovery from a hardware failure and the software failure recovery are described below.

- Confirmation of the entire node

  When it is necessary to refer to this chapter after hardware replacement or as a result of failure determination flowchart* in “Troubleshooting”, refer to Troubleshooting “9.2.2 Confirmation of Recovery from Hardware Failure” (TRBL 09-0610) to check that the entire hardware is in the normal status and there is no other failures.

  *: When it is necessary to refer to this chapter with a SIM (KAQK39XXX-E) of software failure, refer to “Software failure recovery” described below.

- Software failure recovery

  When it is necessary to refer to this chapter after a SIM message (KAQK39XXX-E) concerning a software failure is displayed, refer to Troubleshooting “9.2.3 Recovery Procedure for Software Failure” (TRBL 09-0640) to perform the failure recovery procedure corresponding to the SIM (detail code of KAQK39XXX-E) and the final recovery procedure.

Copyright © 2014, Hitachi, Ltd.

9.2.2 Confirmation of Recovery from Hardware Failure

Figure 9.2.2-1 show the sequence how to check the recovery completion of hardware failure.

Check if all of the hardware are in normal status.

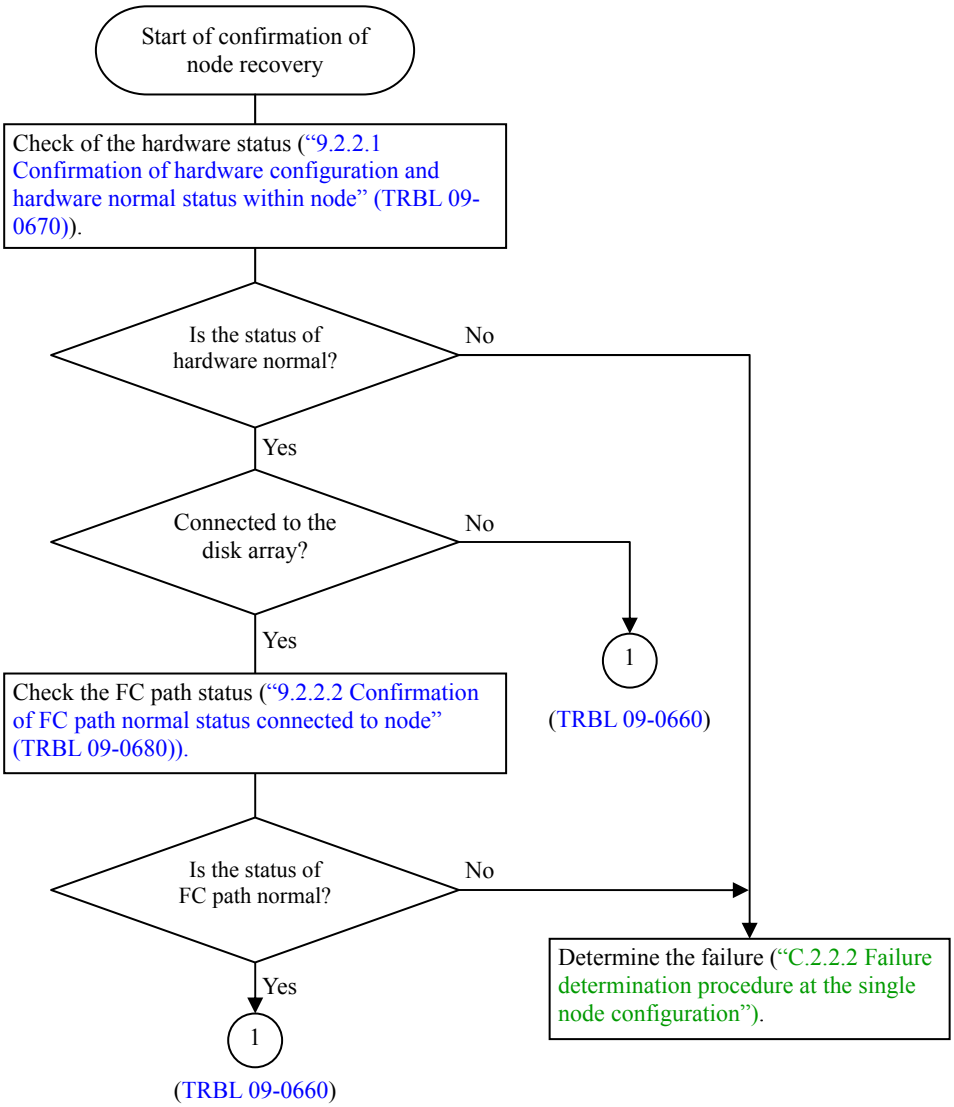


Figure 9.2.2-1 Flow of Hardware Failure Recovery Confirmation (1/3)

Copyright © 2014, Hitachi, Ltd.

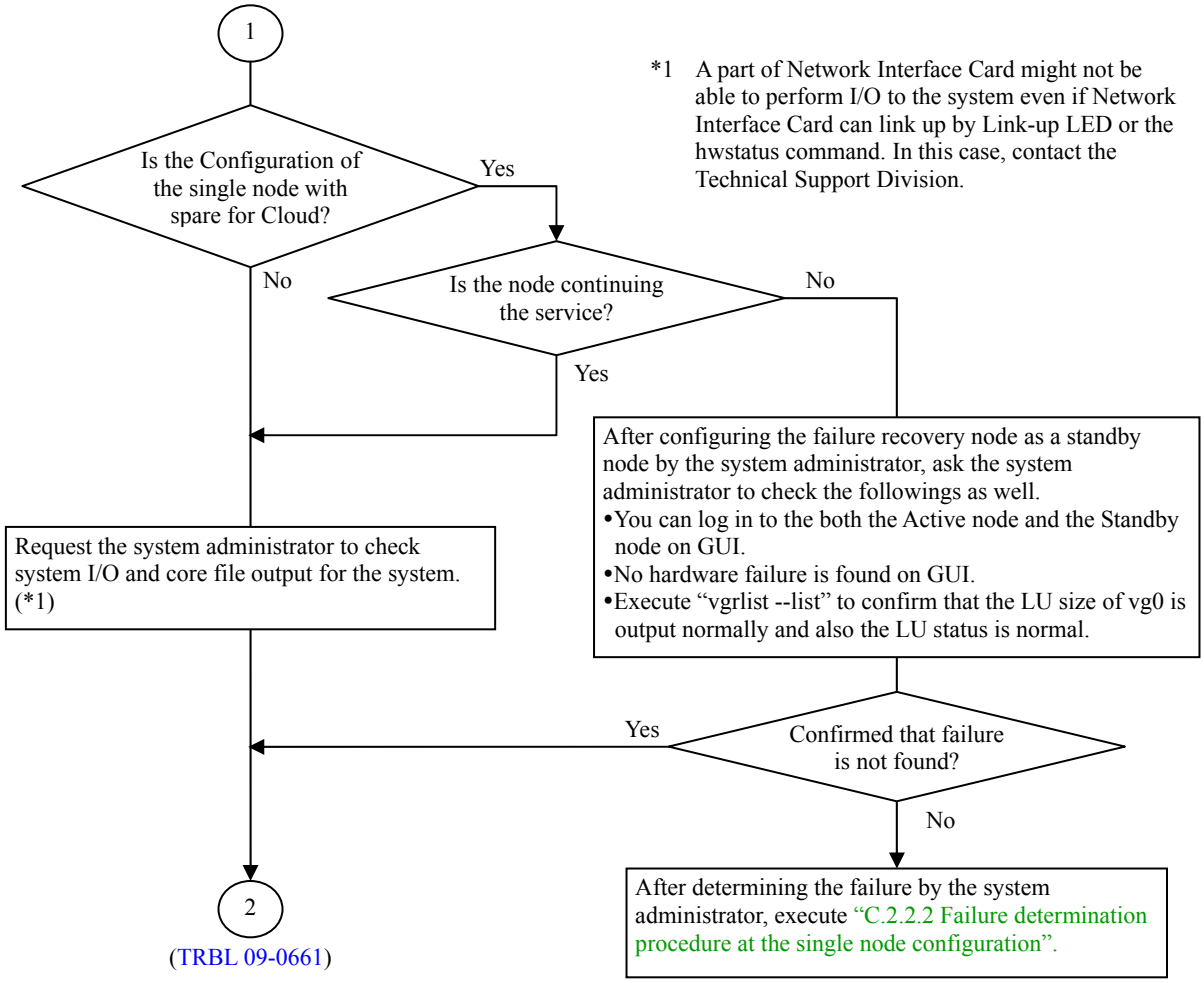


Figure 9.2.2-1 Flow of Hardware Failure Recovery Confirmation (2/3)

Copyright © 2014, 2015, Hitachi, Ltd.

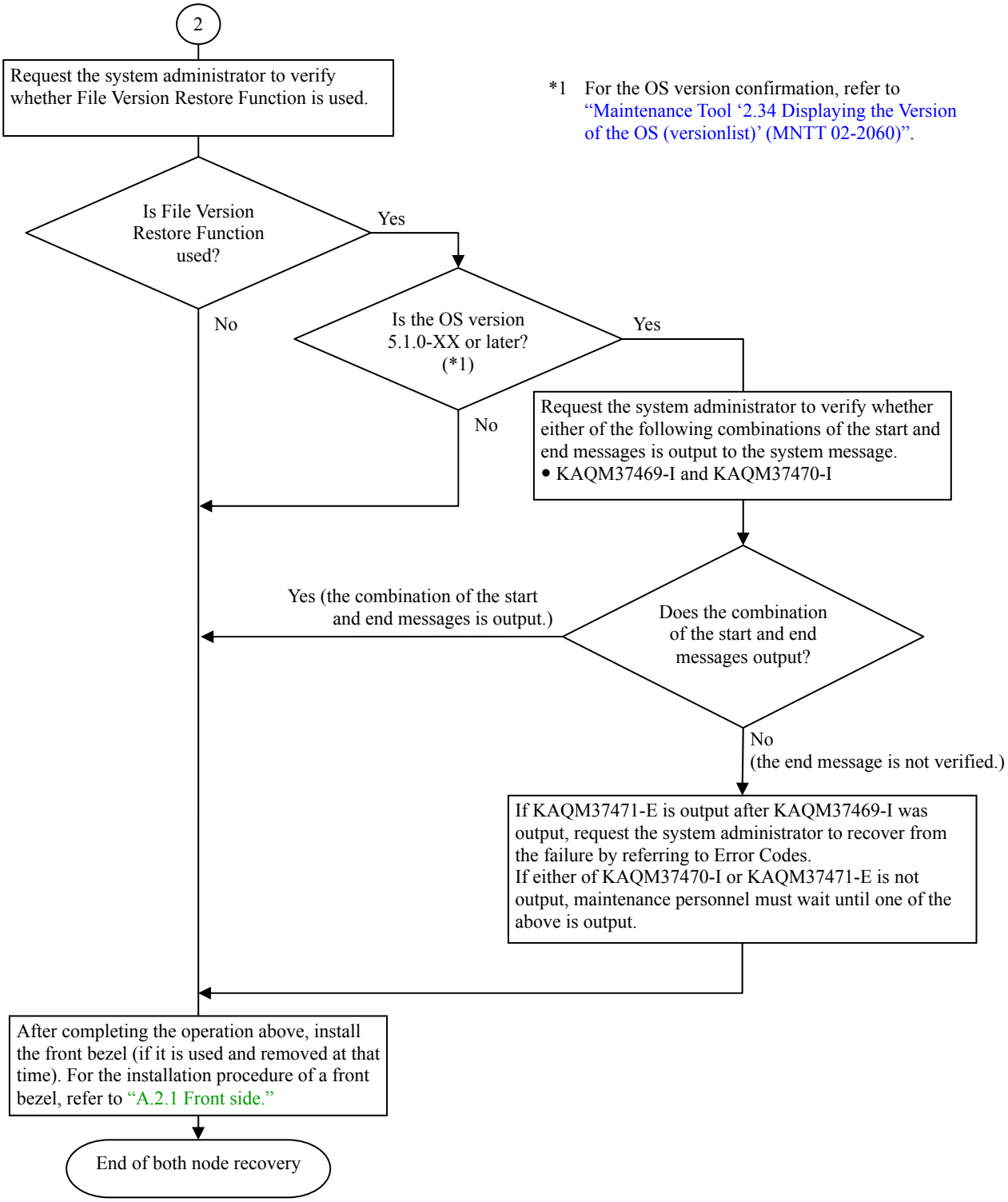


Figure 9.2.2-1 Flow of Hardware Failure Recovery Confirmation (3/3)

Copyright © 2014, Hitachi, Ltd.

9.2.2.1 Confirmation of hardware configuration and hardware normal status within node

Check if all of the hardware within the node is in normal status using "hwstatus" command.

Check if the hardware output results (items of Fan Information, Temperature Information, Power Supply Information, Memory Information, Internal HDD Information, Internal RAID Battery Information, and BMC Information) are “OK” or “installed.” For Network Interface items, check if pm0, mng0 (when a port is used), and ethX* (when a port is used) are “UP”.

*: Provided that the cable is connected. The value of “X” is an integer 0 or greater.

For details about the output result of the hwstatus command, refer to “B.3.1.2 Output format”.

Note: In case of the single node (with standby node) which does not continue the services, a port on the node and the front-end LAN are not connected. Therefore, the link does not show “UP” and the hardware normal status cannot be confirmed.

Confirm the following points.

- If the hardware is HA8000series, perform the HATP (Diagnostic test) for all LAN ports and confirm that no problem exists with them. For the details of HATP, refer to HA8000 Maintenance Manual.
- Execute the iflist command with the –v option and confirm that port names (mng0,ethX⋯) which are used when operating as the Active node are displayed. For the details of the iflist command, refer to “Maintenance Tool ‘2.11 Displaying the Management Port Information (mngiflist)’ (MNTT 02-0800)”.
- Confirm that the LED of LinkUp is turned on by connecting the maintenance PC to the port using the LAN cable owned by the maintenance personnel. However, if the 10GbE port is equipped, contact the system administrator to borrow the 10GbE cable from the customer. If the system administrator cannot borrow the 10GbE cable from the customer, inform that a partial operation check was not able to execute.

A part of Network Interface Card might not be able to perform I/O to the system even if Network Interface Card can link up by Link-up LED or the hwstatus command. In this case, contact the Technical Support Division.

In the case of D51B-2U, run the syseventlist command and confirm that the message related to Internal RAID battery (KAQK37524-W, KAQK37525-E or KAQK37532-E) is not output. For the details, refer to “Maintenance Tool ‘2.6 Displaying SIMs on This Side (syseventlist)’ (MNTT 02-0360)”.

Even if you confirmed that a node does not have a failure on D51B-2U, fault LED on the node might be lit. However it does not have a problem.

Copyright © 2014, 2015, Hitachi, Ltd.

9.2.2.2 Confirmation of FC path normal status connected to node

Check if all of the FC paths within the both nodes are in normal status using "fpstatus" command.

Figure 9.2.2.2-1 shows an example of output result of the fpstatus command execution.

Check if all of the FC paths are in "Online" status.

```
$ sudo fpstatus -v
Path                Target    HostPort HostPortWWN       ArrayPort  ArrayPortWWN     Model  Serial     Status
path000-0002-0A     N0-T000   fc0002   10000000c98f26be  0A         50060e800044b632 AMS    87010001   Online
path000-0003-1B     N0-T000   fc0003   10000000c98f36be  1B         50060e800044b636 AMS    87010001   Online
```

Figure 9.2.2.2-1 Example of Output Result of the fpstatus Command

For details about the output result of the fpstatus command, refer to “Maintenance Tool ‘2.5 Displaying the FC Status (fpstatus)’ (MNTT 02-0280)”.

Copyright © 2014, Hitachi, Ltd.

9.2.3 Recovery Procedure for Software Failure

This section describes the failure recovery procedure and the final recovery procedure for a software failure which occurred during operation of Hitachi Data Ingestor.

Table 9.2.3-1 shows the acquired failure information, the status of Hitachi Data Ingestor, and the section to be referred to for action to be taken (the failure recovery procedure and the final recovery procedure) when a SIM message of software failure is issued. Execute the troubleshooting in reference to the Table 9.2.3-1.

NOTE: The following products are indicated with abbreviations shown on the right to ":".
Hitachi Data Ingestor : HDI

Table 9.2.3-1 List of Software-related Failures (1/2)

#	SIM	Failure	Acquired failure information		HDI status	Recovery method
			core file (*1)	Dump file	Service status	Failure recovery procedure
1	KAQK39500-E Detail=00 00 00 02 Level=00 Type=02	User LU file system is blocked.	N	Y (*2)	All or some services are stopped (*2)	9.2.3.1 Failure recovery when the file system is blocked (TRBL 09-0710)
2	KAQK39500-E Detail=00 00 00 03 Level=00 Type=02	File system in OS area is blocked.	N	N	Service is running.	9.2.3.2 Failure recovery in the case of a OS area failure (TRBL 09-0840)
3	KAQK39500-E Detail=00 02 00 02 Level=00 Type=0A	Mounting of file system to be stored the dump failed.	—	—	—	9.2.5 Software Recovery by Initial OS Installation (TRBL 09-0990)
4	KAQK39500-E Detail=Other than above	—	—	—	—	Acquire the trouble information in reference to Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000). Send the acquired information to the Technical Support Center and request the investigation of the trouble.

Legend: Y: Failure information is output. N: Failure information is not output.

*1: For the core file acquisition, refer to Troubleshooting "6.4 Core Files" (TRBL 06-0050).
*2: Service is available for accesses to other than the blocked file system.

Execute the recovery procedure of failure that corresponds to each SIM. After the recovery procedure of failure, execute the final recovery process as soon as the measurement version of OS is obtained.

Copyright © 2014, Hitachi, Ltd.

Table 9.2.3-1 List of Software-related Failures (2/2)

#	SIM	Failure	Acquired failure information		HDI status	Recovery method	
			core file (*1)	Dump file	Service status	Failure recovery procedure	Final recovery procedure
5	KAQK39601-E Detail=00 00 00 10 Level=00 Type=04	File system mounting failed	N	N	All or some services are stopped.	9.2.3.3 Recovery from KAQK39601-E failure (TRBL 09-0880)	9.2.4 Upgrading the Software by Updating the OS Version (TRBL 09-0970)
	KAQK39601-E Detail=00 00 00 11 Level=00 Type=04	File system unmounting failed					
	KAQK39601-E Detail=00 00 00 20 Level=00 Type=04	Starting NFS sharing failed					
	KAQK39601-E Detail=00 00 00 21 Level=00 Type=04	Terminating NFS sharing failed					
	KAQK39601-E Detail=00 00 00 40 Level=00 Type=04	Starting CIFS failed					
	KAQK39601-E Detail=00 00 00 41 Level=00 Type=04	Stopping CIFS failed					
	KAQK39601-E Detail=00 00 00 50 Level=00 Type=04	Starting File snapshot or File version restore function failed (*2)					
	KAQK39601-E Detail=00 00 00 51 Level=00 Type=04	Stopping File snapshot or File version restore function failed (*2)					
6	KAQK39601-E Detail=00 00 00 F0 Level=00 Type=04	Starting the resource failed	—	—	—	Refer to Troubleshooting "Chapter 6 Acquiring Failure Information" (TRBL 06-0000) and acquire the trouble information. Send the acquired information to the Technical Support Center and request the investigation of the trouble.	
	KAQK39601-E Detail=00 00 00 F1 Level=00 Type=04	Stopping the resource failed					

Legend: Y: Failure information is output. N: Failure information is not output.

*1: Refer to Troubleshooting "6.4 Core Files" (TRBL 06-0050) to get the core file.
*2: HDI does not support File Snapshot.

Follow the failure recovery procedure corresponding to each SIM. After performing the failure recovery procedure, perform the final recovery procedure of troubleshooting as soon as obtaining the update version of the OS.

Copyright © 2014, Hitachi, Ltd.

9.2.3.1 Failure recovery when the file system is blocked

The failure recovery procedure and the recovery method when the file system is blocked are described below.

If a failure occurred when the file system is blocked, execute the failure recovery with the one of following methods depending on the configuration.

Table 9.2.3.1-1 Failure recovery procedure for each configuration

#	Connection to the disk array subsystem	Configuration	Reference
1	Not connected (*1, *2)	Configuration using Management port	Troubleshooting "9.2.3.1.1 Failure recovery of the blocked file system in the Configuration using Management port when not connected to the disk array subsystem" (TRBL 09-0720)
2		Configuration using trunk 2 Data ports	Troubleshooting "9.2.3.1.2 Failure recovery of the blocked file system in the Configuration using trunk 2 Data ports when not connected to the disk array subsystem" (TRBL 09-0730)
3	Connected	Configuration using Management port	Troubleshooting "9.2.3.1.3 Failure recovery of the blocked file system in the configuration connected to the disk array subsystem (TRBL 09-0760)
4		Configuration using trunk 2 Data ports	

*1: In the Configuration of single node with spare for Cloud, if the new installation happens during the procedure, operations after the new installation and management IP address (IP address for the Standby node) setting should be executed by the system administrator.

*2: In the Configuration of single node with spare for Cloud, if the node is not continuing a service, refer to #1.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.1.1 Failure recovery of the blocked file system in the Configuration using Management port when not connected to the disk array subsystem

The failure recovery procedure and the recovery method for the blocked file system in the Configuration using Management port when not connected to the disk array subsystem are described below.

Check the necessity of new installation and the data to be recovered by referring to Table 9.2.3.1.1-1 and execute the failure recovery in the procedures shown in the Table 9.2.3.1.1-2.

Table 9.2.3.1.1-1 Supplementary Table of Failure recovery procedures

#	Model	Failure location	Necessity of new installation	Data to be recovered
1	CR220SM/ D51B-2U	OS area	Execute a new installation without RAID reconfiguration (without user disk initialization)	System LU
2		User area	New installation and setting after the new installation are not necessary	User data (on the failed file system) (*2, *3)
3	Other than above	OS area/User area	Execute a new installation with RAID reconfiguration (with user disk initialization) (*1)	System LU User data (*2)

*1: Entire data in the node is initialized.

*2: Request the system administrator to perform either of the followings.

- Execute fsrepair command (it may take a long time to restore depending on the size and the number of files of the user LU.)
- Delete and re-create the file system, and then restore the data from backup data.

In addition, when the OS version is 4.0.0-XX or later, request to perform the followings.

- Delete and re-create the volume group after completing deletion of the file system (if deletion of the file system was selected.)
- Execute the lumaplist command after completing the replacement of the internal drive to confirm that [size] of user LUs are displayed.

In the case using File snapshot, Active File Migration or Large File Transfer before deletion of the file system, re-set those function at the re-creation of the file system or thereafter.

*3: Be sure to restore the user data from backup data when RAID card is replaced.

Copyright © 2014, 2017, Hitachi, Ltd.

Table 9.2.3.1.1-2 Failure recovery procedures

#	Process	Performed by	Reference
1	Execute the initial OS installation (*1, *3, *4)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
2	Set after completing the installation (*2, *3)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
3	Execute restoration of the data to be recovered confirmed in Table 9.2.3.1.1-1	System administrator	—
4	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
5	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by executing the CLI command open to the system administrator.	System administrator	—
6	Request I/O confirmation for the system	System administrator	—

*1: When meeting the following conditions, KAQM35001-E, KAQM35003-E, and KAQM35007-E messages are output after the initial installation and before the restoration of the system LU, but continue the recovery procedures; you do not need to take measures for the messages.

- The OS version to be initially installed is 4.0.0-XX or later
- Selected user data initialization on the initial installation

*2: In the Configuration of single node with spare for Cloud, a node which is not continuing the service does not require the recovery operations after the step #2. Maintenance personnel needs to contact the system administrator to execute the operations for the Standby node.

*3: Execute this setting if new installation of OS is required in Table 9.2.3.1.1-1.

*4: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2017, Hitachi, Ltd.

9.2.3.1.2 Failure recovery of the blocked file system in the Configuration using trunk 2 Data ports when not connected to the disk array subsystem

The failure recovery procedure and the recovery method for the blocked file system in the Configuration using trunk 2 Data ports when not connected to the disk array subsystem are described below.

Firstly, check the necessity of new installation and the data to be recovered by referring to Table 9.2.3.1.2-1.

Then, ask the system administrator to confirm the location of the free port of the IP-SW which the customer configures. If a free port is available in IP-SW, refer to Table 9.2.3.1.2-2 and if no free port is available, execute the failure recovery in the procedures shown in the Table 9.2.3.1.2-3.

NOTE: When you perform the failure recovery procedures, take a note of the IP address and the Routing that is used at the front-end LAN. These are used at the management port IP address setting after the OS installation.

Table 9.2.3.1.2-1 Supplementary Table of Failure recovery procedures

#	Model	Failure location	Necessity of new installation	Data to be recovered
1	CR220SM/ D51B-2U	OS area	Execute a new installation without RAID reconfiguration (without user disk initialization)	System LU
2		User area	New installation and setting after the new installation are not necessary	User data (on the failed file system) (*2, *3)
3	Other than above	OS area/User area	Execute a new installation with RAID reconfiguration (with user disk initialization) (*1)	System LU User data (*2)

*1: Entire data on the node is initialized.

*2: Request the system administrator to perform either of the followings.

- Execute fsrepair command (it may take a long time to restore depending on the size and the number of files of the user LU.)
- Delete and re-create the file system, and then restore the data from backup data.

In addition, when the OS version is 4.0.0-XX or later, request to perform the followings.

- Delete and re-create the volume group after completing deletion of the file system (if deletion of the file system was selected.)
- Execute the lumaplist command after completing the replacement of the internal drive to confirm that [size] of user LUs are displayed.

In the case using File snapshot, Active File Migration or Large File Transfer before deletion of the file system, re-set those function at the re-creation of the file system or thereafter.

*3: Be sure to restore the user data from backup data when RAID card is replaced.

Copyright © 2014, 2017, Hitachi, Ltd.

Table 9.2.3.1.2-2 Failure recovery procedures (Free Port is Available in IP-SW)

#	Process	Performed by	Reference
1	Connect the free port confirmed with the system administrator and the management port of the node by the LAN cable. (*2)	Maintenance personnel	—
2	Execute the initial OS installation (*1, *2, *3)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
3	Set after completing the installation. (*2) (For the management port IP address, set the IP address and the Routing that are used at the front-end LAN. The IP address and the Routing that are used at the front-end LAN should be confirmed with the system administrator.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
4	Execute restoration of the data to be recovered confirmed in Table 9.2.3.1.2-1	System administrator	—
5	After completing the recovery, remove the LAN cable connected to the management port. (*2)	Maintenance personnel	—
6	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
7	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command open to the system administrator.	System administrator	—
8	Request I/O confirmation for the system	System administrator	—

*1: When meeting the following conditions, KAQM35001-E, KAQM35003-E, and KAQM35007-E messages are output after the initial installation and before the restoration of the system LU, but continue the recovery procedures; you do not need to take measures for the messages.
- The OS version to be initially installed is 4.0.0-XX or later
- Selected user data initialization on the initial installation

*2: Execute this removal if new installation of OS is required in Table 9.2.3.1.2-1.

*3: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2014, 2017, Hitachi, Ltd.

Table 9.2.3.1.2-3 Failure recovery procedures (No Free Port in IP-SW)

#	Process	Performed by	Reference
1	Disable the settings of VLAN/Link aggregation for the IP-SW port connected to a node (*2). (Leaving a note of settings before disabling is necessary)	System administrator	—
2	Remove a LAN cable from a node data port connecting to the IP-SW port which setting was changed by the system administrator and reconnect to the management port. #1 (*2).	Maintenance personnel	—
3	Execute the initial OS installation (*1, *2, *4)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
4	Set after completing the installation. (*2, *3)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
5	Execute restoration of the data to be recovered confirmed in Table 9.2.3.1.2-1	System administrator	—
6	After the completion of recovery, put the LAN cable which was reconnected at the above step #2 back to the original data port (*2).	Maintenance personnel	—
7	Restore the IP-SW settings changed at the above step #1 (VLAN/Link aggregation) (*2).	System administrator	—
8	Confirm that no error message related to the file system or the file sharing is output	System administrator	—
9	In the configuration of HDI for Cloud, confirm if the file configuration is consistent between the HDI and the HCP after performing the restoration by using the CLI command open to the system administrator.	System administrator	—
10	Request I/O confirmation for the system	System administrator	—

*1: When meeting the following conditions, KAQM35001-E, KAQM35003-E, and KAQM35007-E messages are output after the initial installation and before the restoration of the system LU, but continue the recovery procedures; you do not need to take measures for the messages.
- The OS version to be initially installed is 4.0.0-XX or later
- Selected user data initialization on the initial installation

*2: Execute this removal if new installation of OS is required in Table 9.2.3.1.2-1.

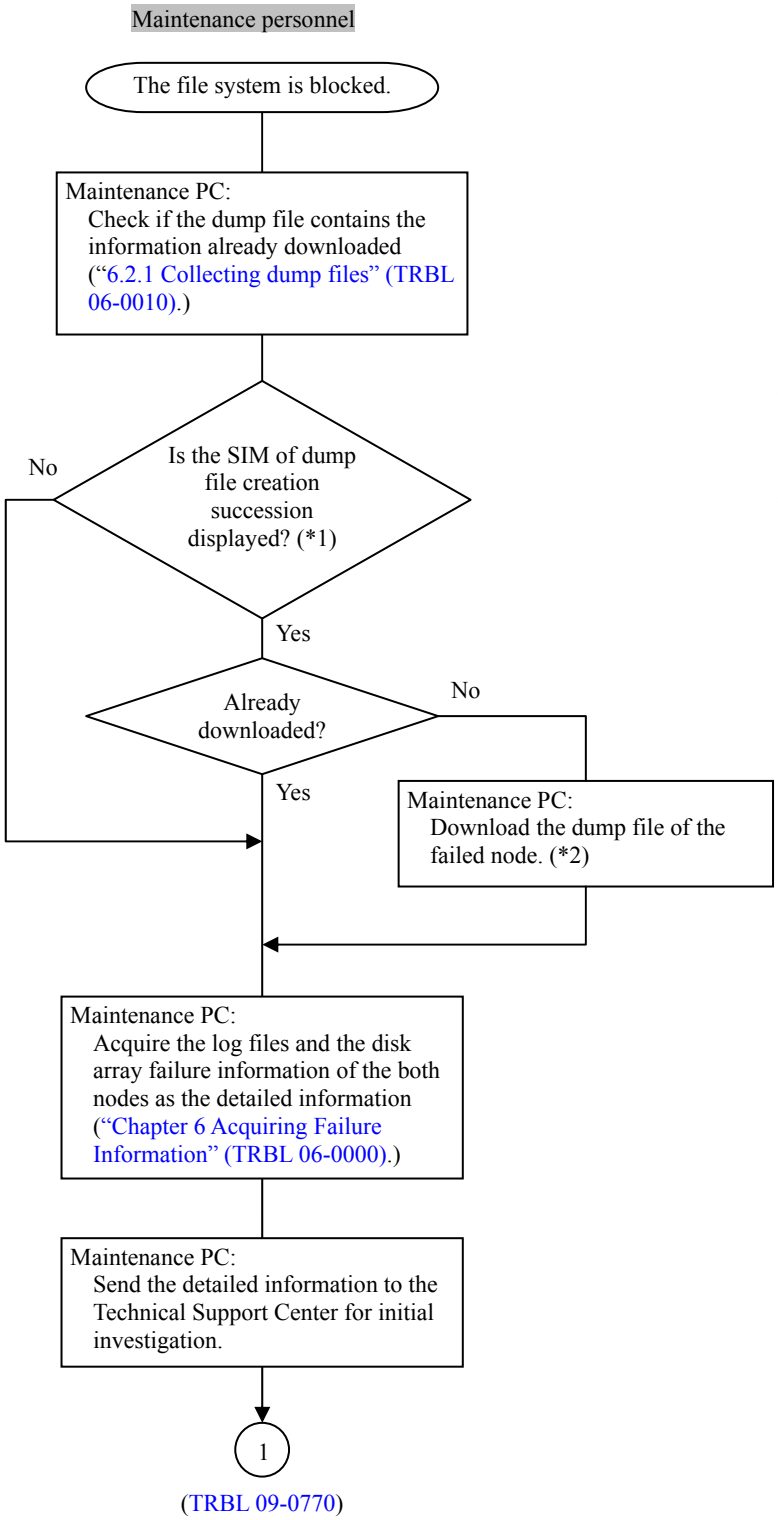
*3: KAQG81003-W will be output after the OS data recovery. However no particular action is required. Continue the recovery procedure.

*4: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.1.3 Failure recovery of the blocked file system in the configuration connected to the disk array subsystem

The failure recovery procedure and the recovery method for the blocked file system in the configuration connected to the disk array subsystem are described below.



*1: Check that SIMs “KAQK39500-E OS error Detail=05 00 00 01 Level=00 Type=03” and “KAQK39528-I Processing to convert dump files ended” are displayed.
*2: Refer to “Maintenance Tool ‘2.21.1 Collecting dump files’ (MNTT 02-1420).”

Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (1/8)

Copyright © 2014, Hitachi, Ltd.

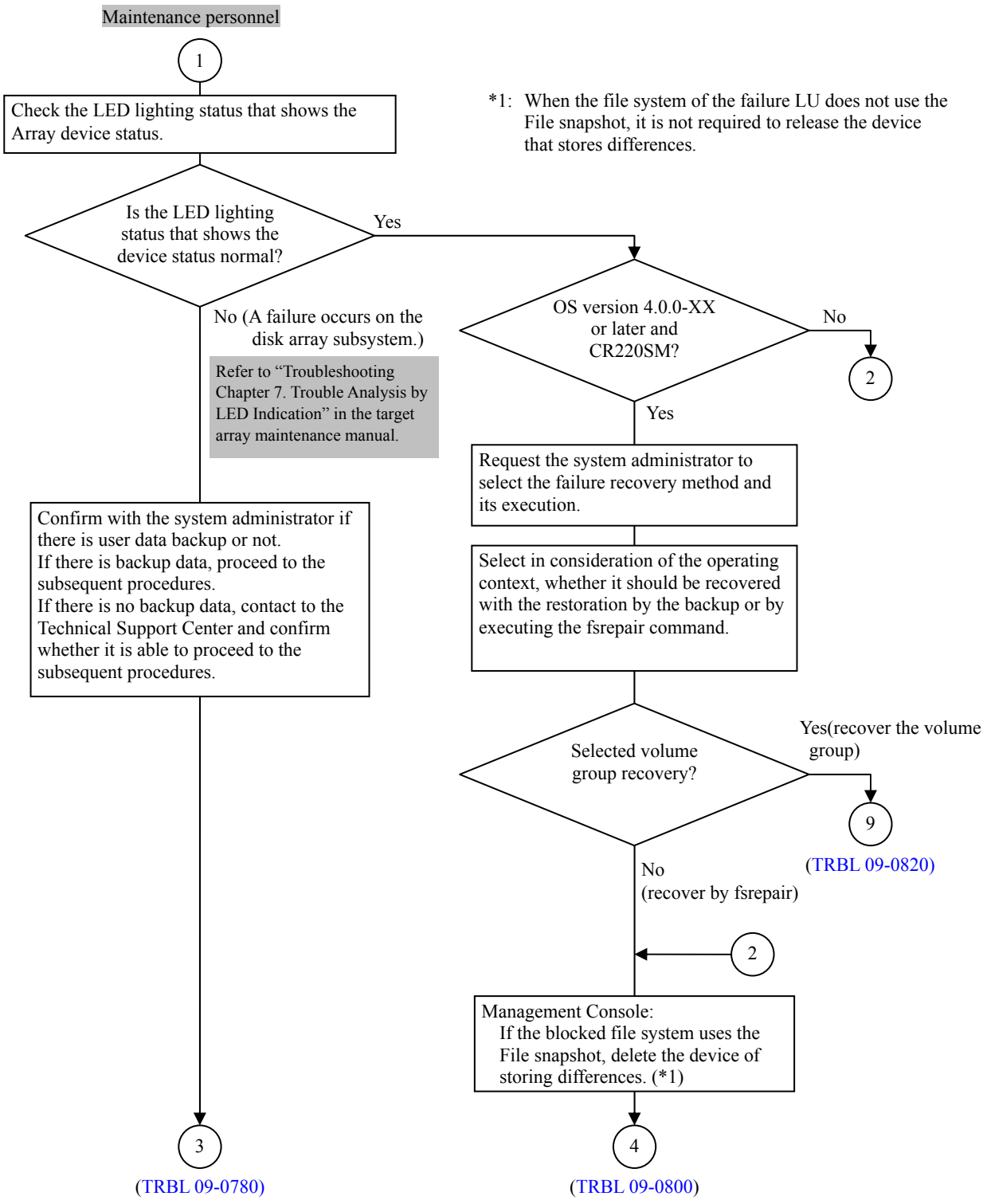
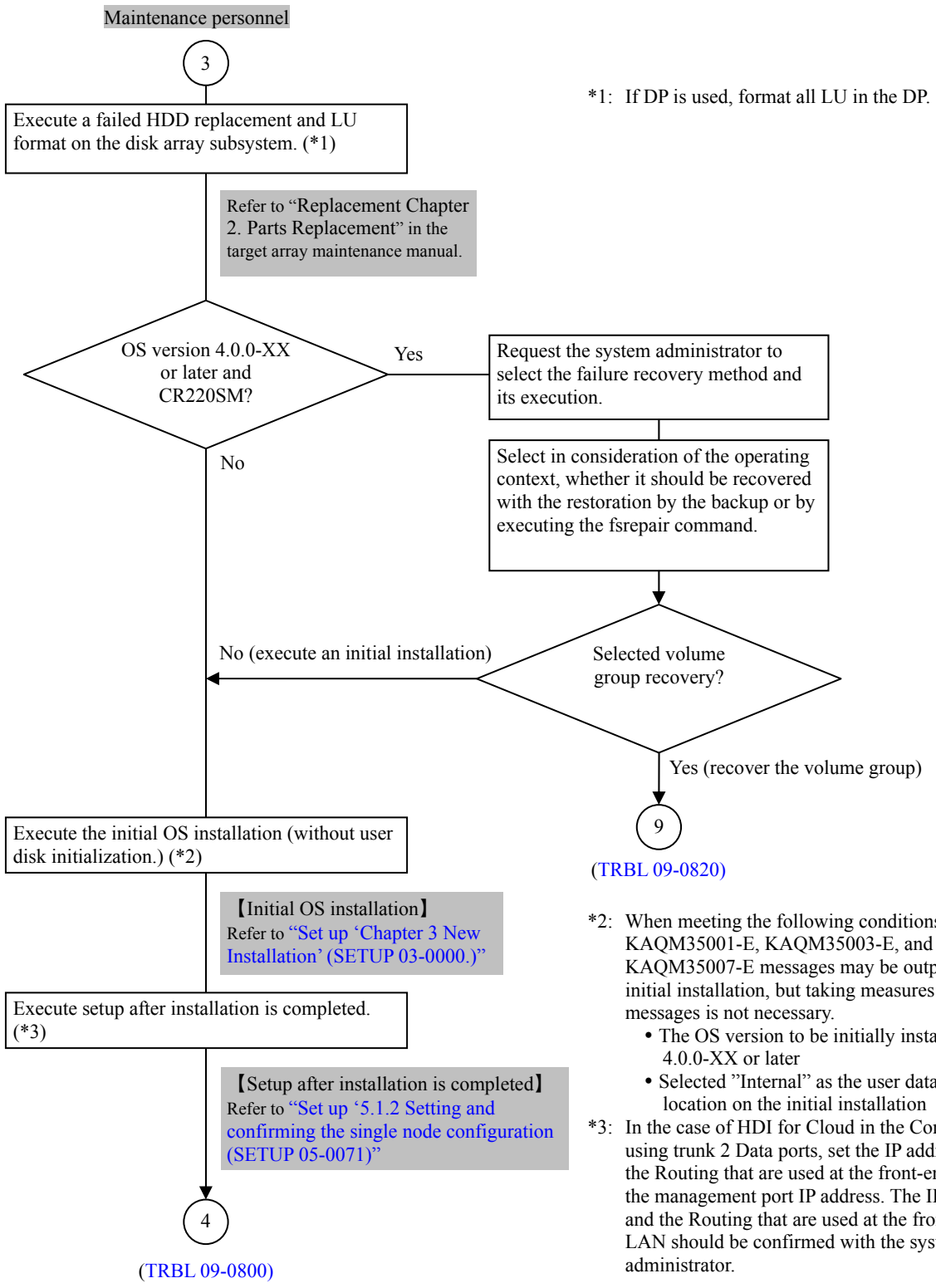


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (2/8)

Copyright © 2014, Hitachi, Ltd.



*1: If DP is used, format all LU in the DP.

*2: When meeting the following conditions, KAQM35001-E, KAQM35003-E, and KAQM35007-E messages may be output after the initial installation, but taking measures for the messages is not necessary.
- The OS version to be initially installed is 4.0.0-XX or later
- Selected "Internal" as the user data storage location on the initial installation

*3: In the case of HDI for Cloud in the Configuration using trunk 2 Data ports, set the IP address and the Routing that are used at the front-end LAN for the management port IP address. The IP address and the Routing that are used at the front-end LAN should be confirmed with the system administrator.

Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (3/8)

Copyright © 2014, Hitachi, Ltd.

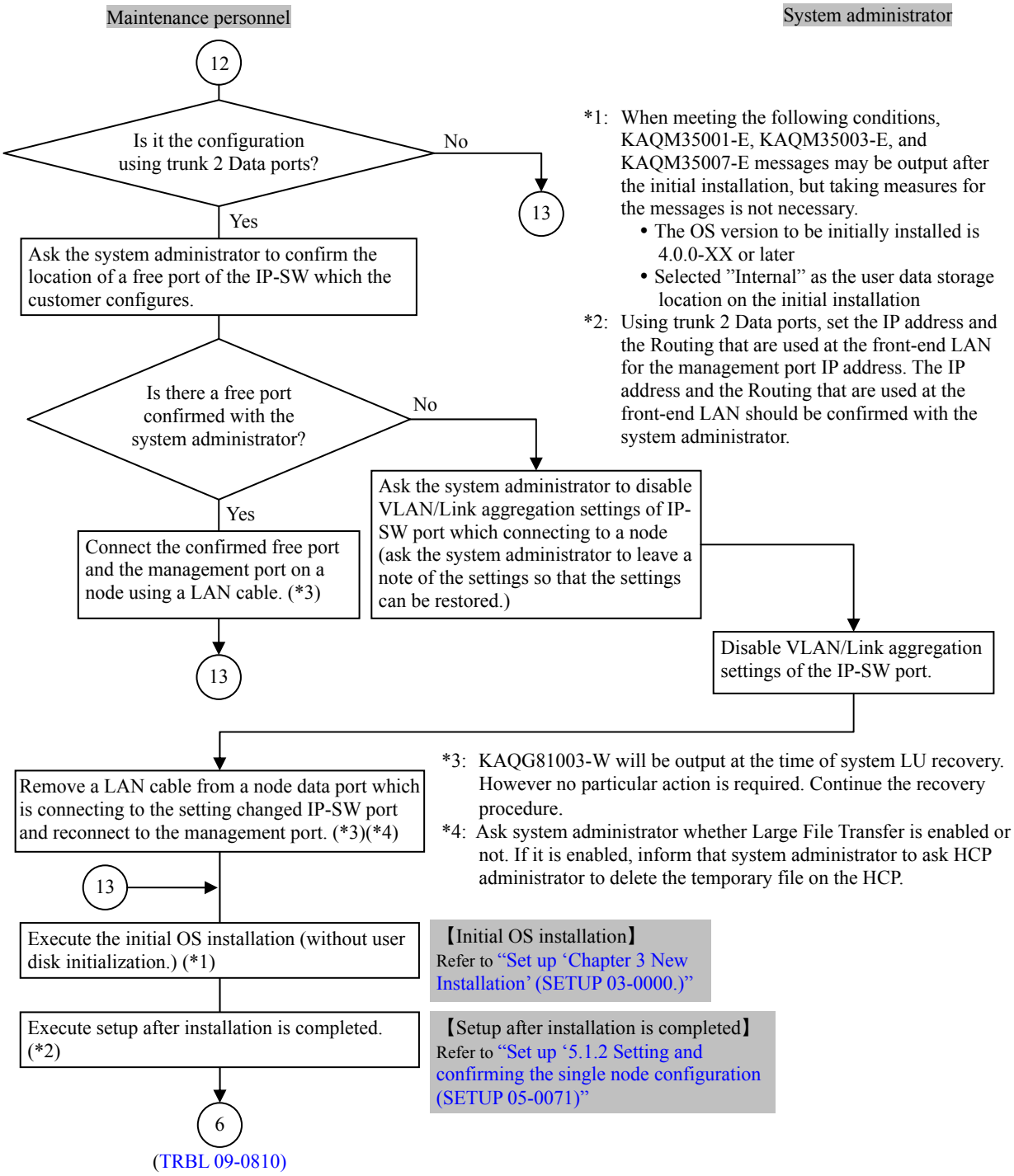


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (4/8)

Copyright © 2014, 2017, Hitachi, Ltd.

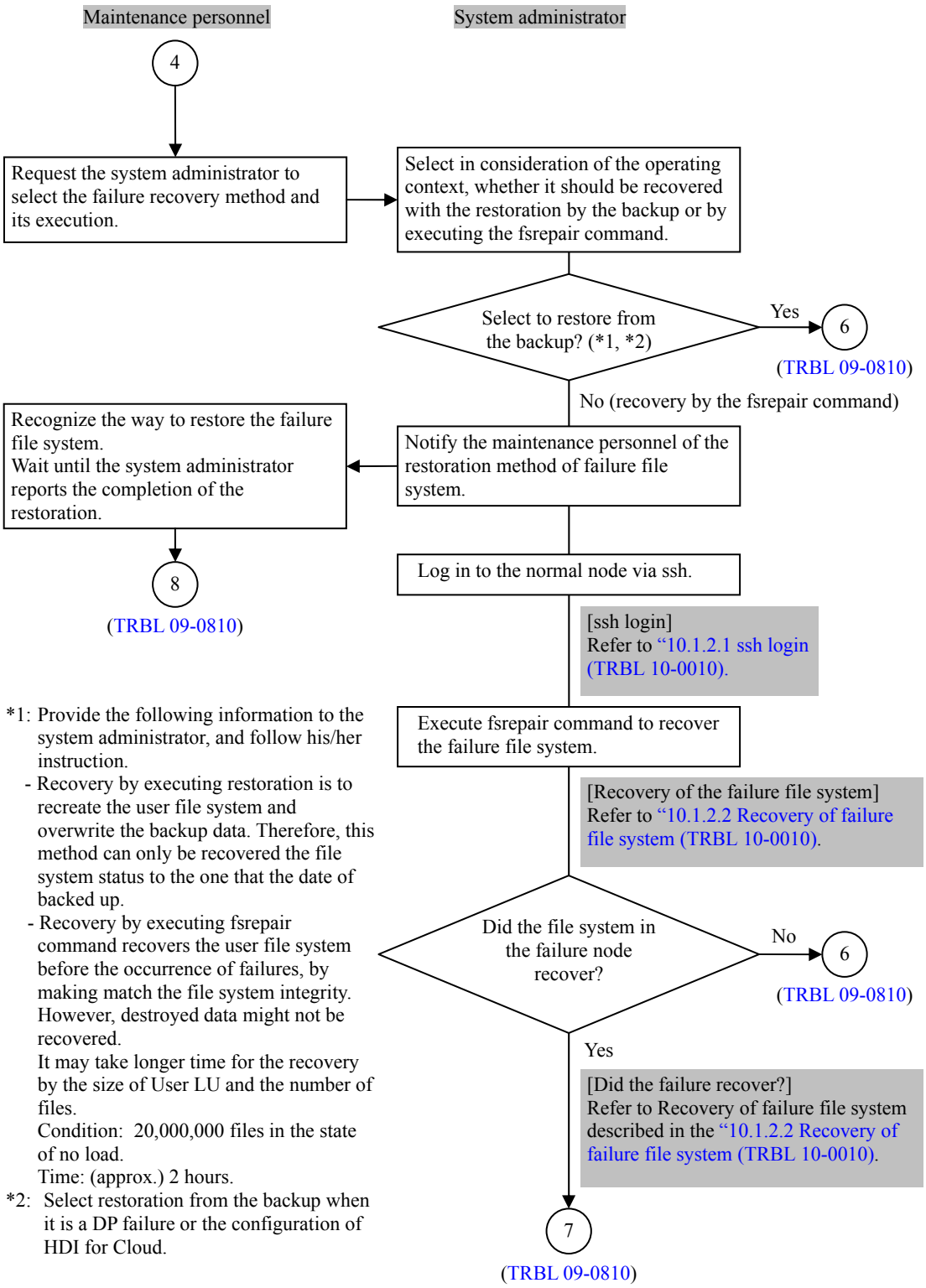


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (5/8)

Copyright © 2014, Hitachi, Ltd.

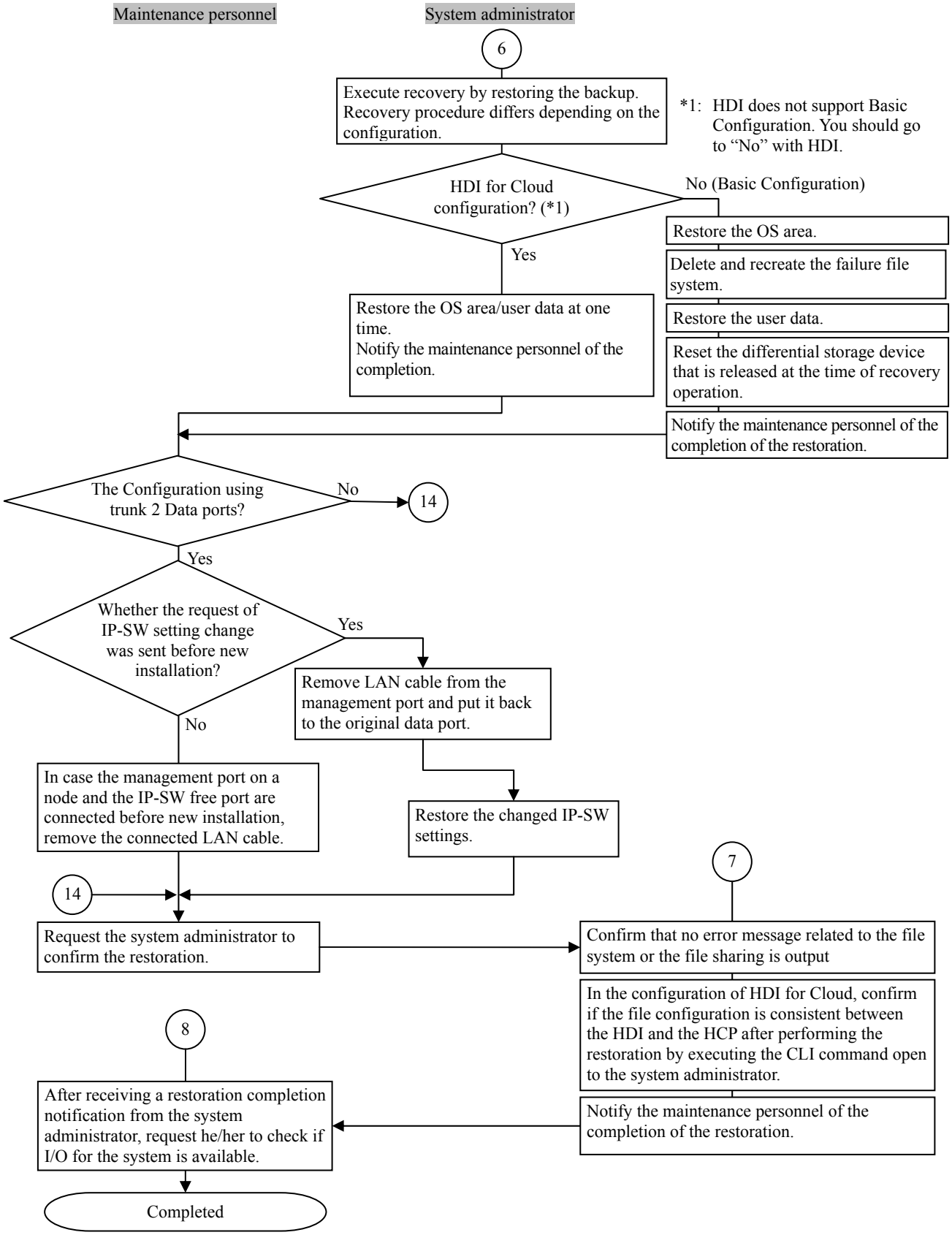


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (6/8)

Copyright © 2014, 2017, Hitachi, Ltd.

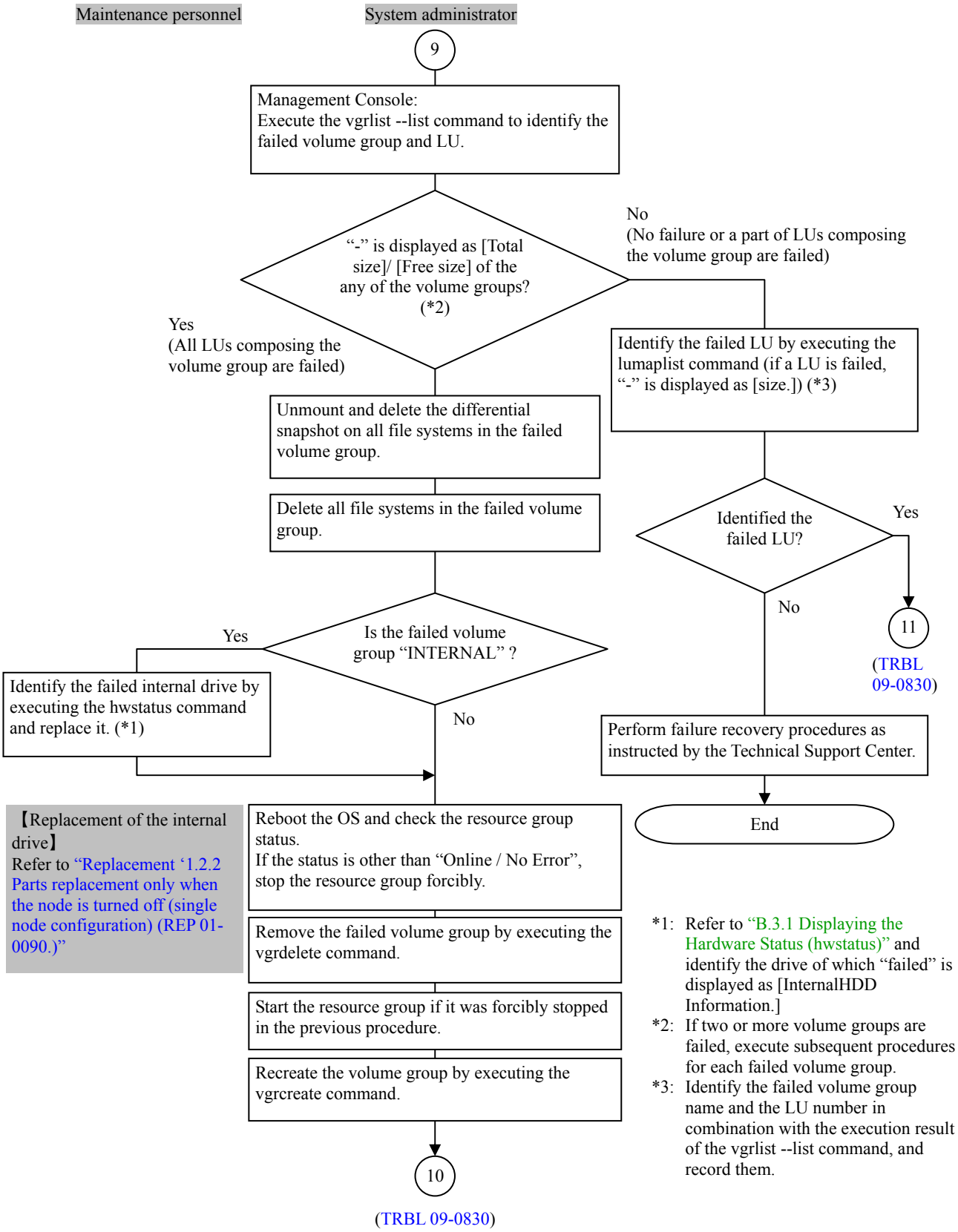


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (7/8)

Copyright © 2014, 2016, Hitachi, Ltd.

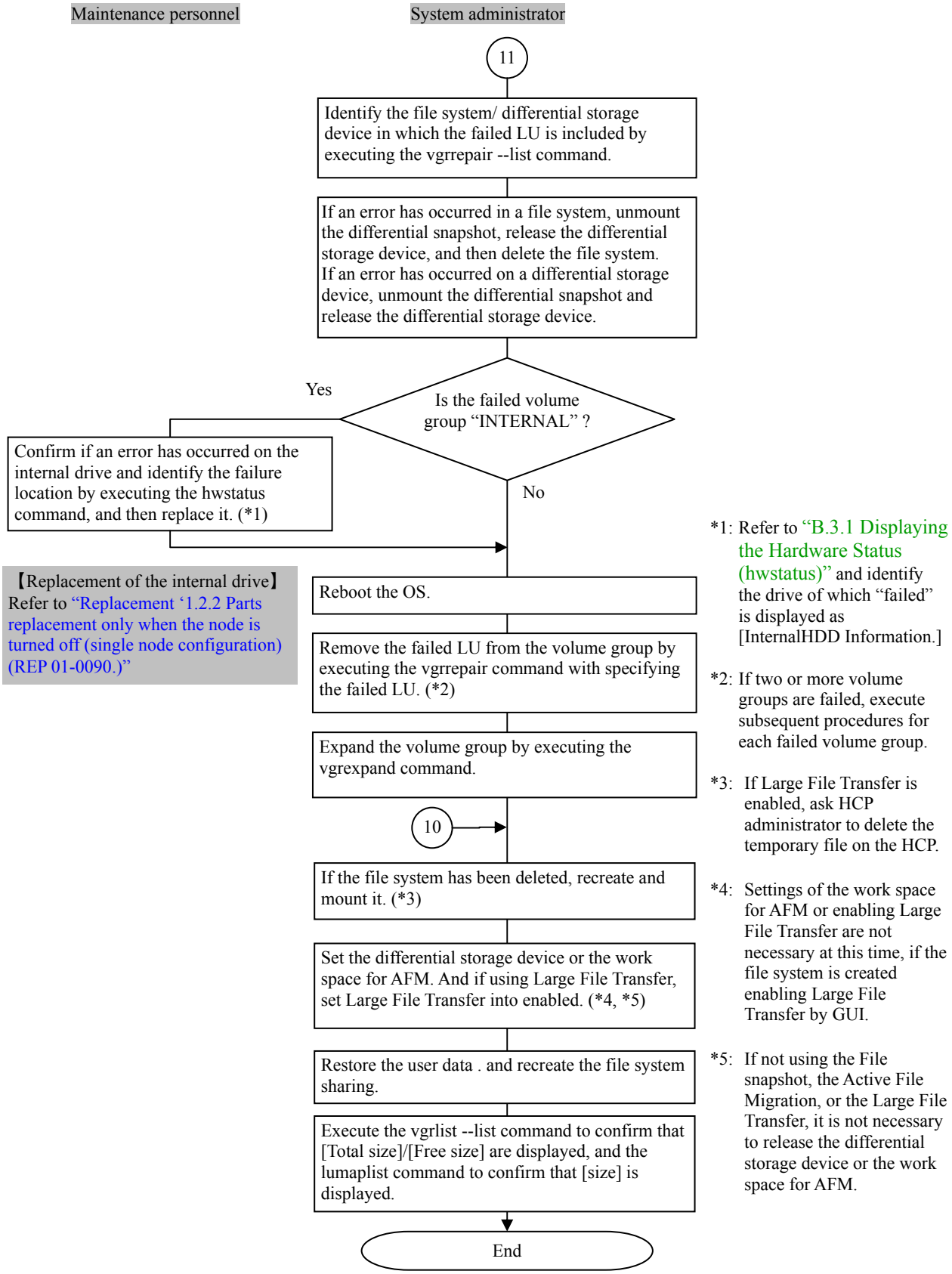


Figure 9.2.3.1.3-1 Recovery Procedure at the time of blocked File System (8/8)

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.2 Failure recovery in the case of a OS area failure

The failure recovery procedure and the recovery method in the case of a failure in the OS area are described below.

When a failure occurred in the OS area, execute the failure recovery with the one of following methods depending on the configuration.

Table 9.2.3.2-1 Failure recovery procedure for each configuration

#	Connection to the disk array subsystem	Configuration	Reference
1	Not connected (*1, *2)	Configuration using Management port	Troubleshooting "9.2.3.1.1 Failure recovery of the blocked file system in the Configuration using Management port when not connected to the disk array subsystem" (TRBL 09-0720)
2		Configuration using trunk 2 Data ports	Troubleshooting "9.2.3.1.2 Failure recovery of the blocked file system in the Configuration using trunk 2 Data port when not connected to the disk array subsystem" (TRBL 09-0730)
3	Connected	Configuration using Management port	Troubleshooting "9.2.3.2.1 Failure recovery of the OS area in the Configuration using Management port when connected to the disk array subsystem" (TRBL 09-0850)
4		Configuration using trunk 2 Data ports	Troubleshooting "9.2.3.2.2 Failure recovery of the OS area in the Configuration using trunk 2 Data ports when connected to the disk array subsystem" (TRBL 09-0860)

*1: In the Configuration of single node with spare for Cloud, if the new installation happens during the procedure, operations after the new installation and management IP address (IP address for the Standby node) setting should be executed by the system administrator.

*2: In the Configuration of single node with spare for Cloud, if the node is not continuing a service, refer to #1.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.2.1 Failure recovery of the OS area in the Configuration using Management port when connected to the disk array subsystem

The failure recovery procedure and the recovery method for the OS area in the configuration using the management port when connected to the disk array subsystem are described below.

Execute the failure recovery in the procedures shown in the Table 9.2.3.2.1-1.

Table 9.2.3.2.1-1 Failure recovery procedures

#	Process	Performed by	Reference
1	Execute the initial OS installation (without RAID reconfiguration) (*1, *2)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
2	Set after completing the installation	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
3	Execute the restoration of the OS area (recovery of user data is not required)	System administrator	—
4	Request I/O confirmation for the system	system administrator	—

*1: Because there is no failure in the user data on the disk array subsystem.

*2: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.2.2 Failure recovery of the OS area in the Configuration using trunk 2 Data ports when connected to the disk array subsystem

The failure recovery procedure and the recovery method for the OS area in the configuration using trunk 2 data ports when connected to the disk array subsystem are described below.

Ask the system administrator for the location of a free port of the IP-SW which the customer configures and execute the failure recovery in the following either of procedures depending on the situation.

- In case IP-SW has a free port, refer to Table 9.2.3.2.2-1.
- In case IP-SW does not have a free port, refer to Table 9.2.3.2.2-2.

NOTE: Before performing the failure recovery procedures, obtain the IP address and the Routing that is used in the link aggregation from the system administrator. These are used at the management port IP address setting after the OS installation.

Table 9.2.3.2.2-1 Failure recovery procedures (Free Port is Available in IP-SW)

#	Process	Performed by	Reference
1	Connect the confirmed free port and the Management port of the node by the LAN cable.	Maintenance personnel	—
2	Execute the initial OS installation (without RAID reconfiguration) (*1, *2)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
3	Set after completing the installation (Set the IP address and the Routing that are used in the link aggregation for the management port IP address. The IP address and the Routing that are used in the link aggregation should be confirmed with the system administrator.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
4	Execute the restoration of the OS area (recovery of user data is not required)	System administrator	—
5	After completing the recovery, remove the LAN cable connected to the management port.	Maintenance personnel	—
6	Request I/O confirmation for the system	System administrator	—

*1: Because there is no failure in the user data on the disk array subsystem.
*2: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2014, 2017, Hitachi, Ltd.

Table 9.2.3.2.2-2 Failure recovery procedures (Free Port is not Available in IP-SW)

#	Process	Performed by	Reference
1	Disable the settings of VLAN/Link aggregation for the IP-SW port connected to a node. (Leaving a note of settings before disabling is necessary)	System administrator	—
2	Remove a LAN cable from a node data port connecting to the IP-SW port which was disabled at the above step #1 and reconnect to the management port.	Maintenance personnel	—
3	Execute the initial OS installation (without RAID reconfiguration) (*1, *3)	Maintenance personnel	"Set up 'Chapter 3 New Installation' (SETUP 03-0000)"
4	Set after completing the installation (Set the IP address and the Routing that are used in the link aggregation for the management port IP address. The IP address and the Routing that are used in the link aggregation should be confirmed with the system administrator.)	Maintenance personnel	"Set up '5.1 Setting/Confirmation after New Installation' (SETUP 05-0000)"
5	Execute the restoration of the OS area (recovery of user data is not required) (*2)	System administrator	—
6	After the completion of recovery, put the LAN cable which was reconnected at the above step#2 back to the original data port.	Maintenance personnel	—
7	Restore the IP-SW settings changed at the above step #1 (VLAN/Link aggregation) (*2).	System administrator	—
8	Request I/O confirmation for the system	System administrator	—

*1: Because there is no failure in the user data on the disk array subsystem.
*2: KAQG81003-W will be output after the OS data recovery. However, no particular action is required. Continue the recovery procedure.
*3: Ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.3 Recovery from KAQK39601-E failure

The failure recovery procedure and the recovery method corresponding to the KAQK39601-E message are described below.
The SIM message KAQK39601-E shows detail codes corresponding to different failures. Identify the failure content by referring to the detail code.
Table 9.2.3.3-1 describes the detail codes and failure details of the KAQK39601-E message. Also it shows the sections to be referred to for recovery procedure.

Table 9.2.3.3-1 Detail Codes of KAQK39601-E and Failure Content

#	SIM and detail code	Meaning	Failure Content	Recovery procedure (*1)
1	KAQK39601-E Detail=00 00 00 10 Level=00 Type=04	File system mounting failed	File system failure	• 9.2.3.3.1 (TRBL 09-0890) • 9.2.3.3.2 (TRBL 09-0920)
	KAQK39601-E Detail=00 00 00 11 Level=00 Type=04	File system unmounting failed		
2	KAQK39601-E Detail=00 00 00 20 Level=00 Type=04	Starting NFS sharing failed	Start/Terminate of NFS sharing failure	• 9.2.3.3.1 (TRBL 09-0890) • 9.2.3.3.3 (TRBL 09-0930)
	KAQK39601-E Detail=00 00 00 21 Level=00 Type=04	Terminating NFS sharing failed		
3	KAQK39601-E Detail=00 00 00 40 Level=00 Type=04	Starting CIFS failed	CIFS Start/Stop failure	• 9.2.3.3.1 (TRBL 09-0890) • 9.2.3.3.4 (TRBL 09-0940)
	KAQK39601-E Detail=00 00 00 41 Level=00 Type=04	Stopping CIFS failed		
4	KAQK39601-E Detail=00 00 00 50 Level=00 Type=04	Starting File snapshot or File version restore function failed (*2)	File snapshot or File version restore function Start/Stop failure	• 9.2.3.3.1 (TRBL 09-0890) • 9.2.3.3.5 (TRBL 09-0960)
	KAQK39601-E Detail=00 00 00 51 Level=00 Type=04	Stopping File snapshot or File version restore function failed (*2)		

*1 Recovery procedure branches into several branches in Flow (A) of Troubleshooting "Figure 9.2.3.3.1-1" (TRBL 09-0890). After branching, proceed to a flowchart corresponding to the type of failure (9.2.3.3.2 to 9.2.3.3.5) and execute the recovery procedure according to the flowchart. When the recovery procedure of each flowchart is completed, return to Flow (B) of Troubleshooting "Figure 9.2.3.3.1-1" (TRBL 09-890) to execute the recovery procedures of service confirmation.
*2 HDI does not support Snapshot.

For the final recovery after the recovery procedure of KAQK39601-E, perform the procedure of Troubleshooting "9.2.4 Upgrading the Software by Updating the OS Version" (TRBL 09-0770).

NOTE: Check if any of the #2, #3, #4 detail codes is output together with the #1 detail code. If the #1 detail code is output, perform the #1 recovery procedure.

The flowchart of the failure recovery procedure shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status.

Copyright © 2014, 2017, Hitachi, Ltd.

9.2.3.3.1 Procedure for KAQK39601-E failure recovery

The failure recovery procedure for the KAQK39601-E message is described below in the form of a flowchart.

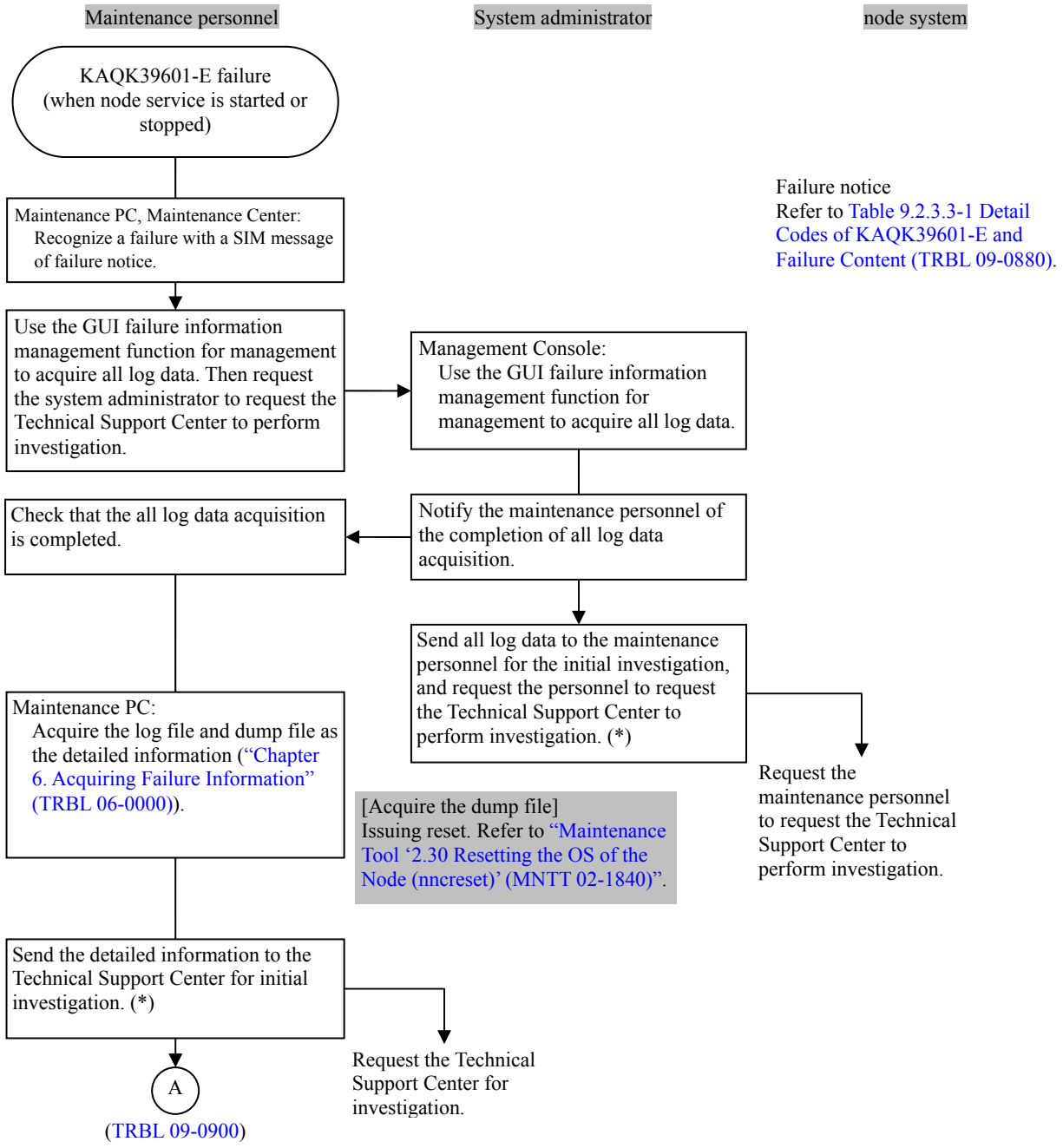


Figure 9.2.3.3.1-1 Procedure for KAQK39601-E Failure Recovery (1/3)

Copyright © 2014, Hitachi, Ltd.

Maintenance personnel | System administrator | node system

A

Perform any of the following failure recovery procedures (sections to be referred to) according to the failure content.

#	SIM and detail code	Failure Content	Next recovery procedure
1	KAQK39601-E Detail=00 00 00 10 Level=00 Type=04 or Detail=00 00 00 11 Level=00 Type=04	File system failure	• 9.2.3.3.2 (TRBL 09-0920)
2	KAQK39601-E Detail=00 00 00 20 Level=00 Type=04 or Detail=00 00 00 21 Level=00 Type=04	Start/Terminate of NFS sharing failure	• 9.2.3.3.3 (TRBL 09-0930)
3	KAQK39601-E Detail=00 00 00 40 Level=00 Type=04 or Detail=00 00 00 41 Level=00 Type=04	CIFS Start/Stop failure	• 9.2.3.3.4 (TRBL 09-0940)
4	KAQK39601-E Detail=00 00 00 50 Level=00 Type=04 or Detail=00 00 00 51 Level=00 Type=04	File snapshot or File version restore function Start/Stop failure	• 9.2.3.3.5 (TRBL 09-0960)

After completing the recovery procedure of the referred-to section, execute the next procedure of Troubleshooting “Figure 9.2.3.3.1-1 Procedure for KAQK39601-E Failure Recovery (3/3)” (TRBL09-0910).

B

(TRBL 09-0910)

Figure 9.2.3.3.1-1 Procedure for KAQK39601-E Failure Recovery (2/3)

Copyright © 2014, Hitachi, Ltd.

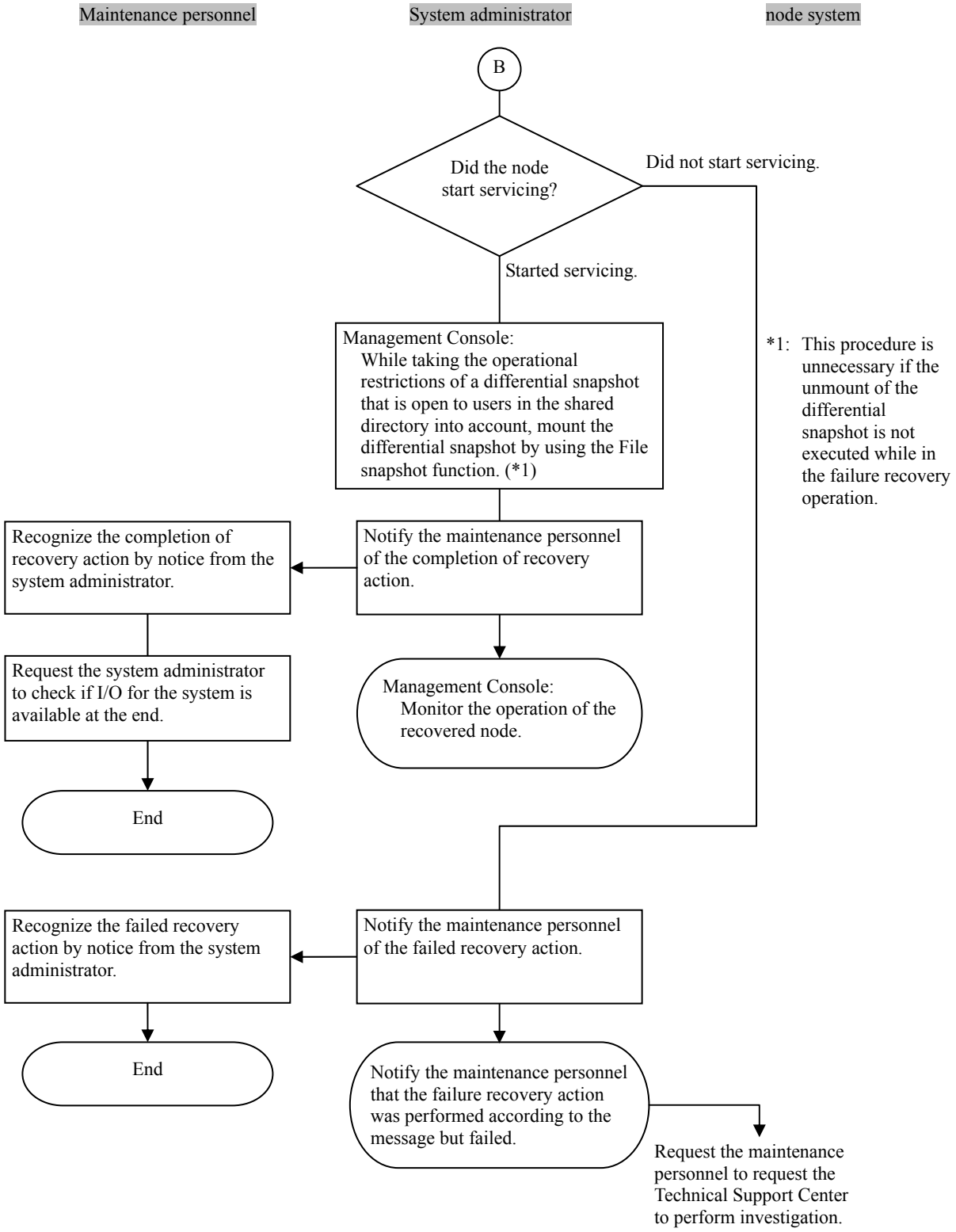


Figure 9.2.3.3.1-1 Procedure for KAQK39601-E Failure Recovery (3/3)

Copyright © 2014, Hitachi, Ltd.

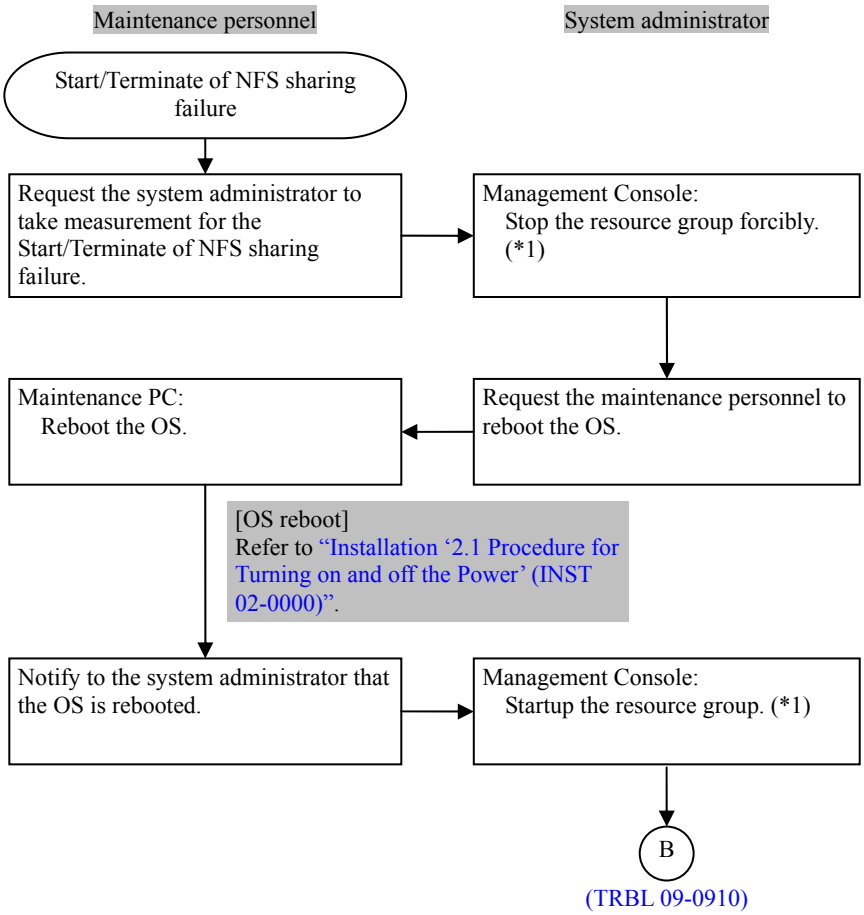
9.2.3.3.2 File system failures

For the failure recovery method of the file system failure, refer to Troubleshooting “9.2.3.1 Failure recovery when the file system is blocked” (TRBL 09-0710).

Copyright © 2014, Hitachi, Ltd.

9.2.3.3.3 Start/Terminate of NFS sharing failures

The next flowchart shows the failure recovery of Start/Terminate of NFS sharing failure.



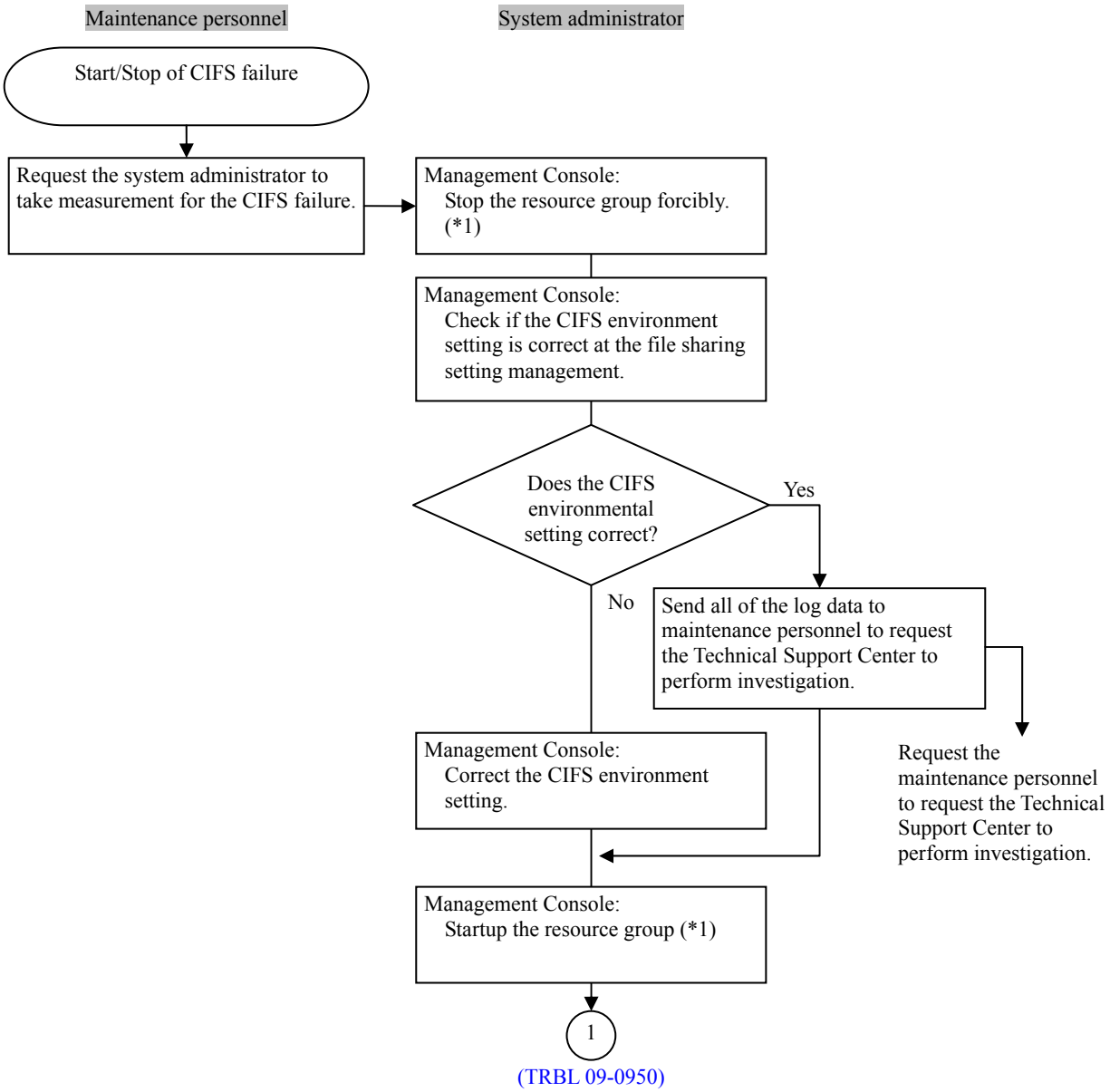
*1: If the system administrator is absent, maintenance personnel should ask the system administrator to have a permission to execute the start/stop of the resource group. Execute the command after the system administrator gives a notice to end users.
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".
- For the stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)".

Figure 9.2.3.3.3-1 Procedure for Start/Terminate of NFS Sharing Failure Recovery

Copyright © 2014, Hitachi, Ltd.

9.2.3.3.4 CIFS Start/Stop failures

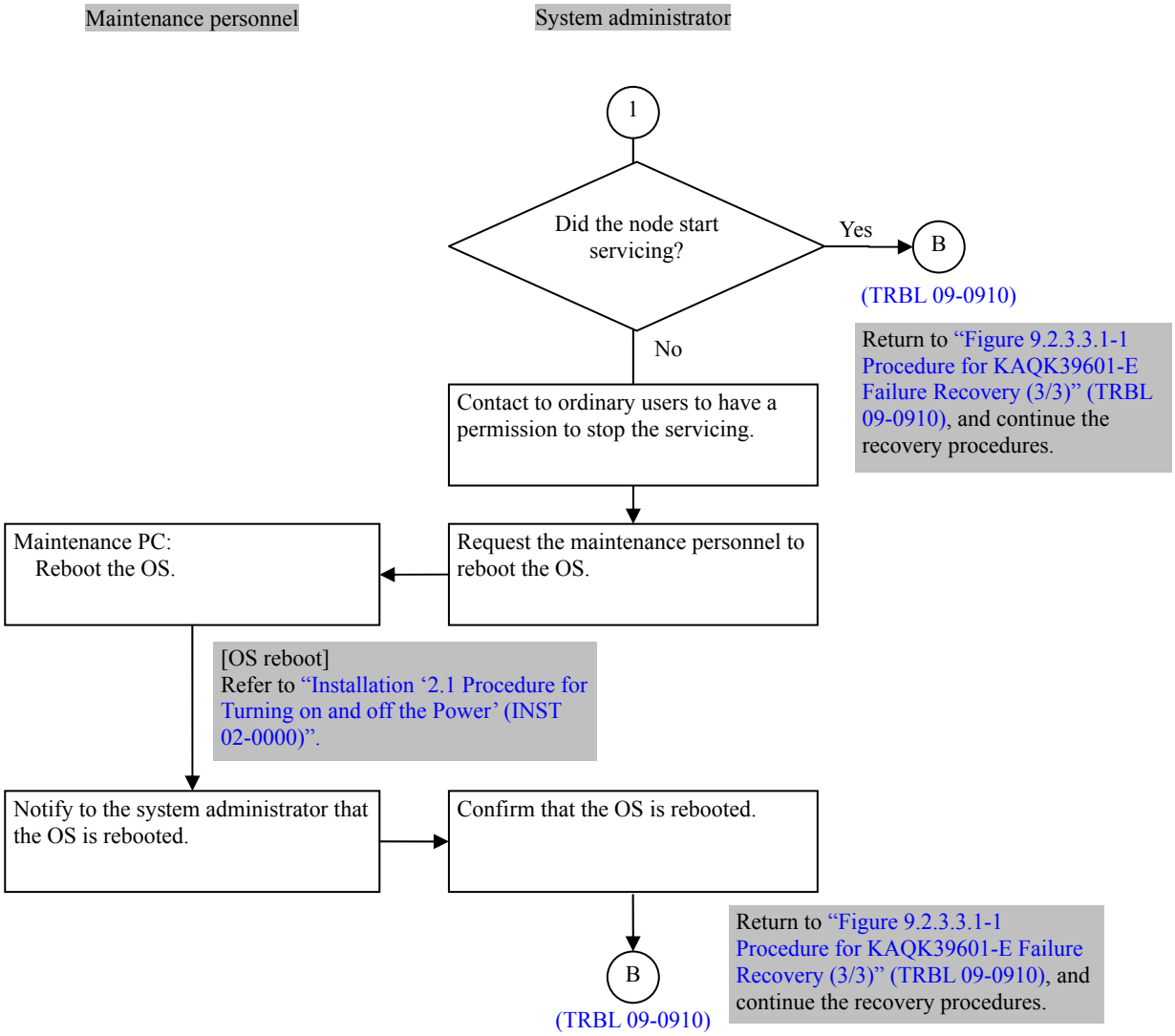
The next flowchart shows the failure recovery of Start/Stop of CIFS failure.



*1: If the system administrator is absent, maintenance personnel should ask the system administrator to have a permission to execute the start/stop of the resource group. Execute the command after the system administrator gives a notice to end users.
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".
- For the stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)".

Figure 9.2.3.3.4-1 Procedure for Start/Stop of CIFS Failure Recovery (1/2)

Copyright © 2014, Hitachi, Ltd.



*1: If the system administrator is absent, maintenance personnel should ask the system administrator to have a permission to execute the start/stop of the resource group. Execute the command after the system administrator gives a notice to end users.
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".
- For the stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)".

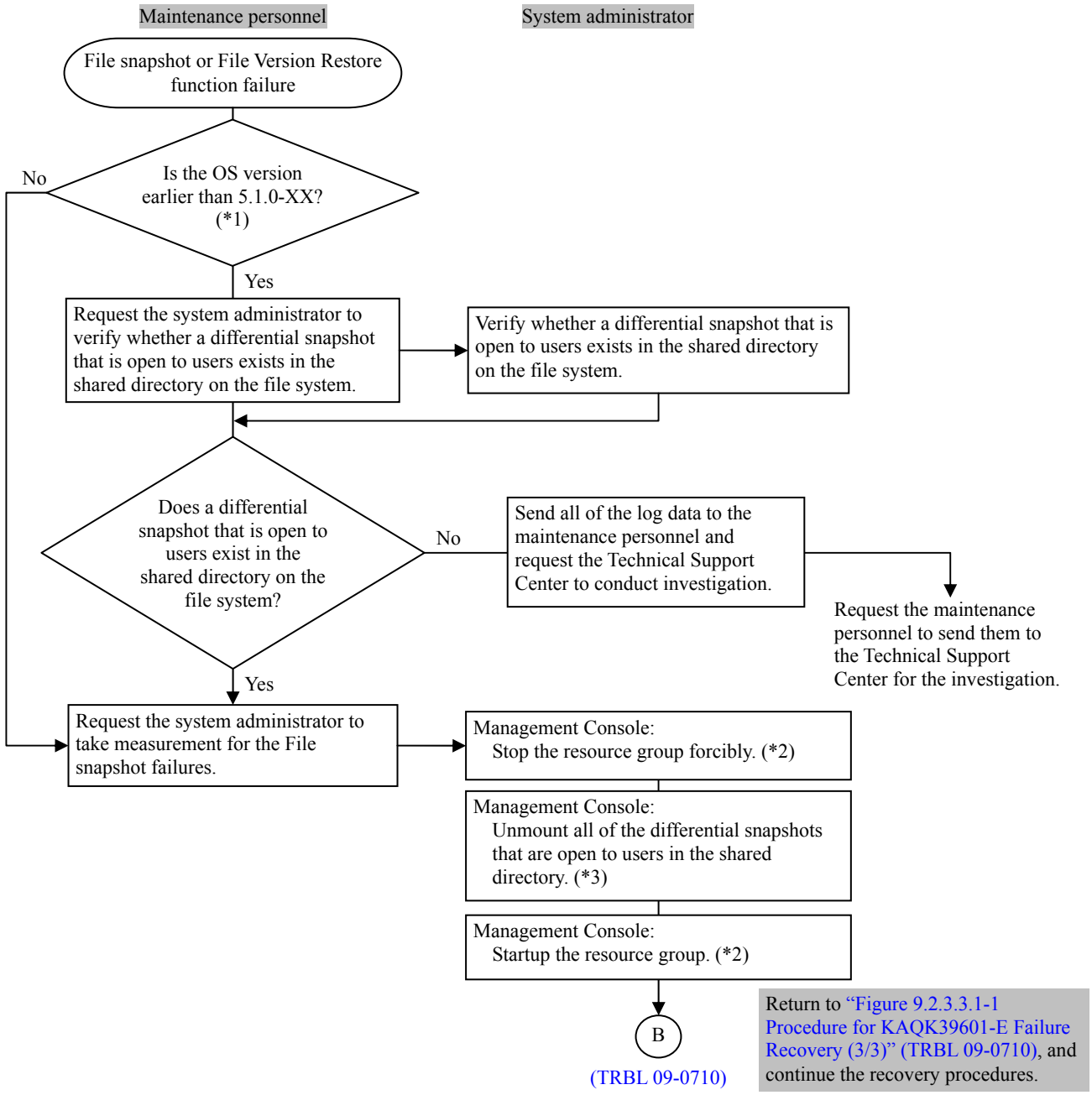
Figure 9.2.3.3.4-1 Procedure for Start/Stop of CIFS Failure Recovery (2/2)

Copyright © 2014, Hitachi, Ltd.

9.2.3.3.5 File snapshot or File Version Restore function failure

This section describes the recovery procedure for the File snapshot or File Version Restore function failure in the form of a flowchart.

NOTE: HDI does not support Snapshot.



*1: For the OS version confirmation, refer to "Maintenance Tool '2.34 Displaying the Version of the OS (versionlist)' (MNTT 02-2060)"
*2: If the system administrator is absent, maintenance personnel should ask the system administrator to have a permission to execute the start/stop of the resource group. Execute the command after the system administrator gives a notice to end users.
- For the startup of the resource group, refer to "Maintenance Tool '2.52 Resource group Starts Up (rgstart)' (MNTT 02-2870)".
- For the stop of the resource group, refer to "Maintenance Tool '2.53 Stopping Resource group (rgstop)' (MNTT 02-2950)".

*3: Execute this procedure when File snapshot is used. This procedure is unnecessary if File snapshot is not used.

Figure 9.2.3.3.5-1 Procedure for File snapshot or File Version Restore Function Failure Recovery

Copyright © 2014, Hitachi, Ltd.

9.2.4 Upgrading the Software by Updating the OS Version

As the final recovery procedure for KAQK39500-E or KAQK39601-E, update the OS version to upgrade the software.

This section describes the procedure to upgrade the software by updating the OS version.

Table 9.2.4-1 provides the overview of the software upgrading by updating the OS version.

Table 9.2.4-1 Procedure of Software Upgrading by Updating the OS Version

Procedure	Process	Remarks
1	Obtain the update version (OS).	—
2	Stop the OS.	—
3	Update the OS to upgrade the software.	—
4	Return the automatic save setting of the system LU to the setting before the failure occurrence.	—

The flowchart shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status. Upgrading procedures for the maintenance personnel and the system administrator are shown respectively.

Copyright © 2014, Hitachi, Ltd.

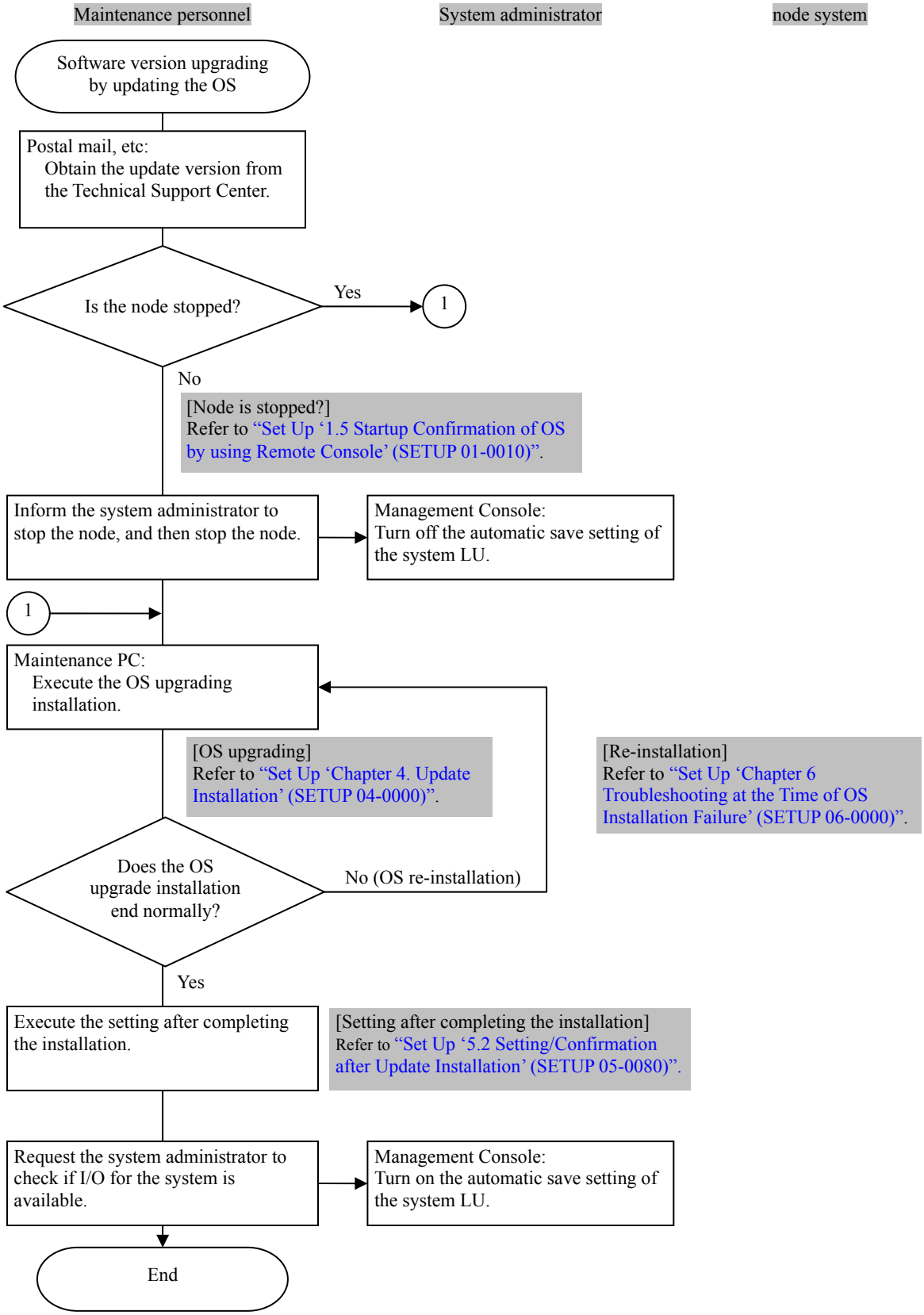


Figure 9.2.4-1 Upgrading the Software by Updating the OS Version

Copyright © 2014, 2016, Hitachi, Ltd.

9.2.5 Software Recovery by Initial OS Installation

As the failure recovery procedure for KAQK39500-E Detail=00 02 00 02, execute the initial OS installation.

This section describes the procedure to execute the initial OS installation.

Table 9.2.5-1 and Table 9.2.5-2 provides the overview of the re-installation of the software by the initial OS installation.

Table 9.2.5-1 Procedure of Initial OS Installation when not connected to the disk array subsystem

Procedure	Process	Remarks
1	Stop the node.	—
2	Execute a new OS installation. (*1, *2, *4, *5)	—
3	Request the system administrator to restore the whole data. (*3)	In the configuration of HDI for Cloud, the data can be restored at one time.
4	Return the automatic save setting of the system LU to the setting before the failure occurrence.	—

*1: In the case of CR220SM/ D51B-2U, select “without RAID reconfiguration (without user disk initialization.)”
In the case of other than CR220SM/ D51B-2U, select “with RAID reconfiguration (with user disk initialization.)”
*2: If "with RAID reconfiguration” is selected, the whole data on the node will be initialized.
*3: In the case of CR220SM/ D51B-2U, request to restore the system LU.
*4: In the Configuration of single node with spare for Cloud, a node which is not continuing the service does not require the recovery operations after the step #2. Maintenance personnel needs to contact the system administrator to execute the operations for the Standby node.
*5: If the user data restoration has executed in step #3, ask system administrator whether Large File Transfer is enabled or not. If it is enabled, inform that system administrator to ask HCP administrator to delete the temporary file on the HCP.

Table 9.2.5-2 Procedure of Initial OS Installation when connected to the disk array subsystem

Procedure	Process	Remarks
1	Stop the node.	—
2	Execute the initial OS installation without RAID reconfiguration.	The user data on the disk array subsystem is not initialized.
3	Request the system administrator to restore the OS area.	Restoration of the user data is not required.
4	Return the automatic save setting of the system LU to the setting before the failure occurrence.	—

The flowchart shows the manner how the maintenance personnel cooperates with the system administrator to grasp the node system status. Initial installation procedure of OS for the maintenance personnel and the system administrator are shown respectively.

Copyright © 2014, 2017, Hitachi, Ltd.

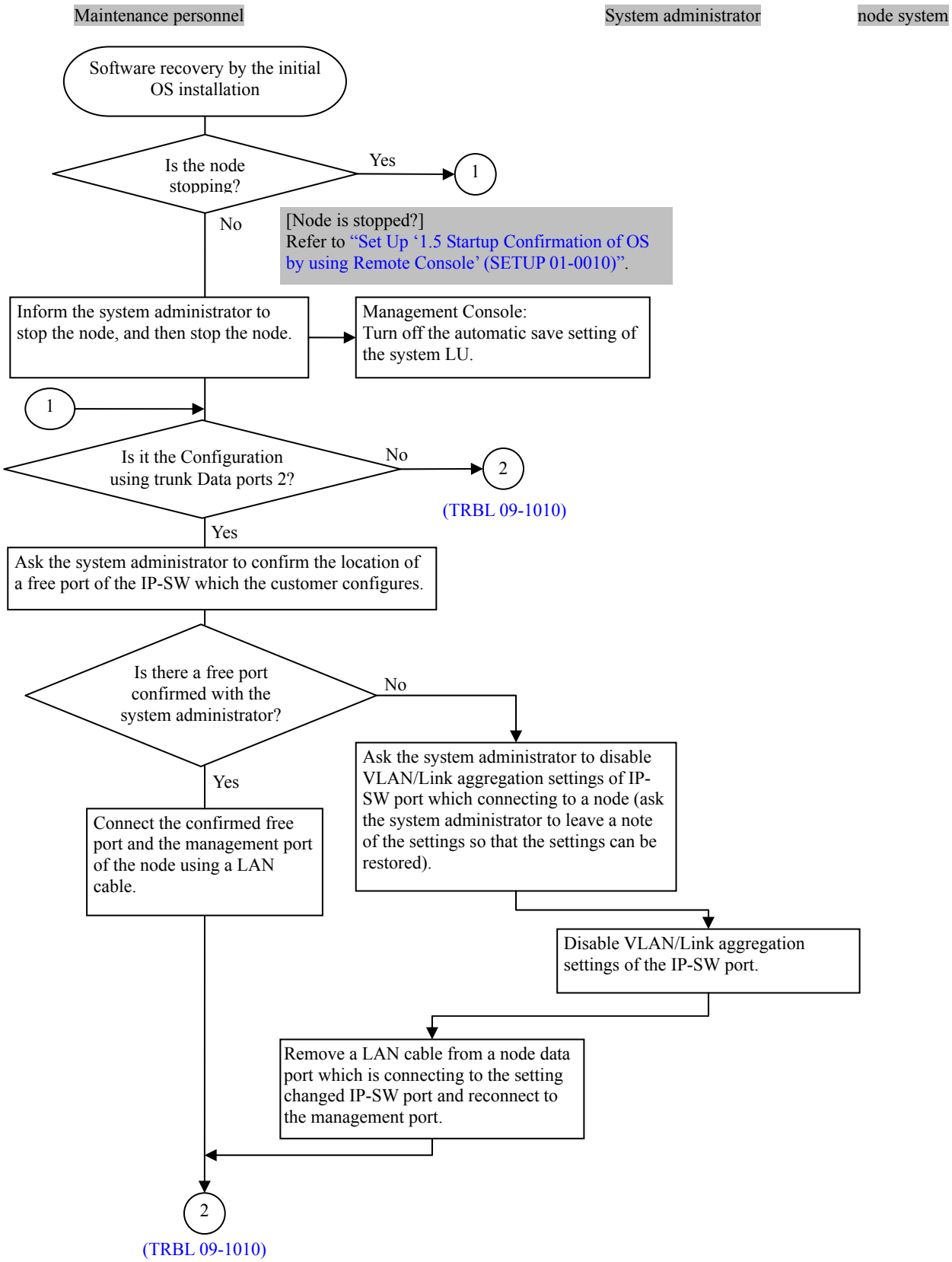
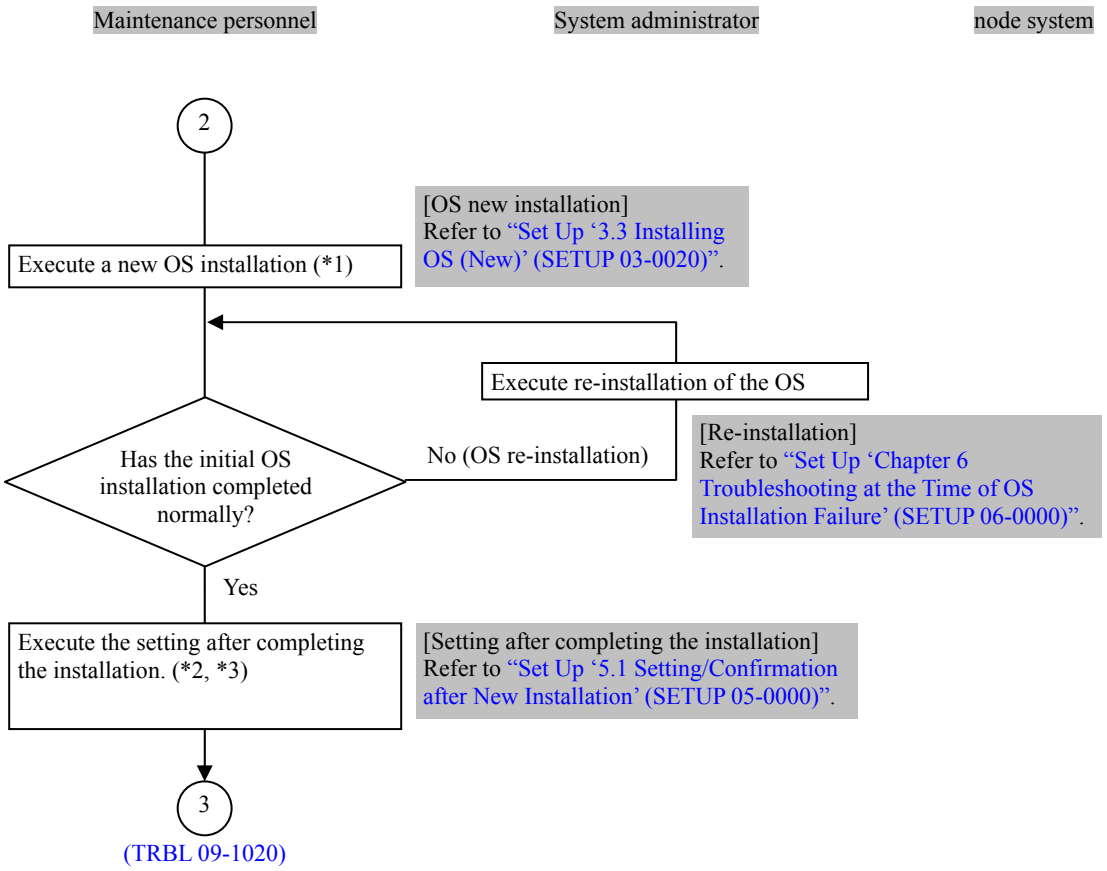


Figure 9.2.5-1 Recovery of the software by the initial OS installation (1/3)

Copyright © 2014, Hitachi, Ltd.



*1: For confirming the necessity of RAID reconfiguration, refer to the following table.

Connected to the disk array subsystem	CR220SM and D51B-2U	Other than CR220SM and D51B-2U
Yes	—	without RAID reconfiguration (without user disk initialization)
No	without RAID reconfiguration (without user disk initialization)	with RAID reconfiguration (with user disk initialization)

*2: Set after completing the installation
(In the case of Configuration using trunk 2 Data ports, if the management port and a IP-SW free port are connected before the installation, set the IP address and routing used in the link aggregated port to the Management port. Ask system administrator about the IP address and routing information of link aggregated port.)

*3: In the Configuration of the single node with spare for Cloud, a node which is not continuing the service does not require the recovery operations after the next page of this manual. Maintenance personnel needs to contact the system administrator to execute the operations for the Standby node

Figure 9.2.5-1 Recovery of the software by the initial OS installation (2/3)

Copyright © 2014, 2015, Hitachi, Ltd.

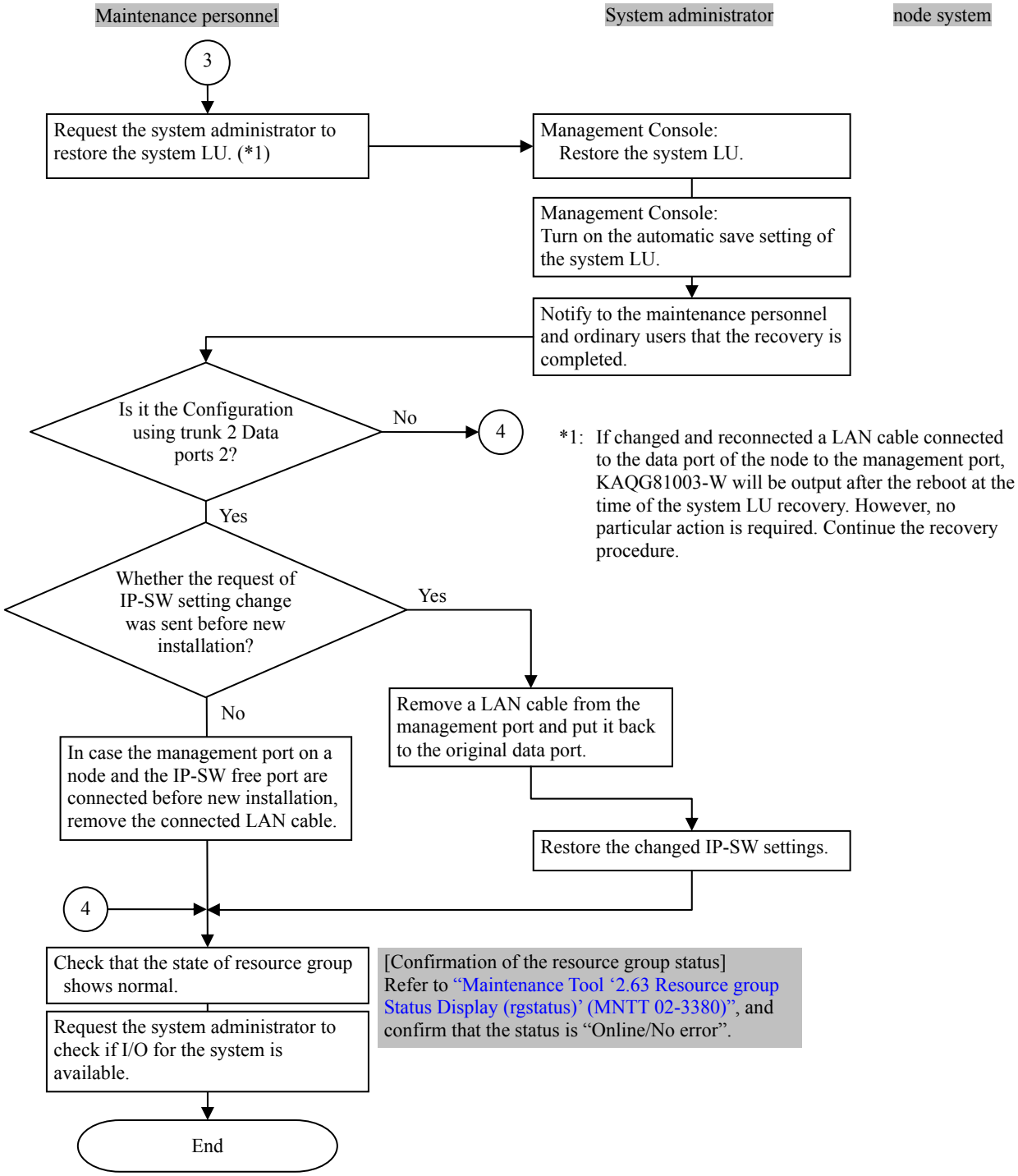


Figure 9.2.5-1 Recovery of the software by the initial OS installation (3/3)

Copyright © 2014, 2017, Hitachi, Ltd.

Chapter 10 Appendix A fsrepair Command

10.1 Overview

The fsrepair command to be used for the recovery at the time of file system blockade and the operation method are shown. Request the system administrator to execute the fsrepair command according to the procedure described in the maintenance manual.

NOTE:
- The environment to enable ssh login is required in the management console. Request the system administrator to prepare for the environment to enable ssh login from the management console. Furthermore, do not perform the operation (including failover and cluster stop) for the file system during fsrepair command execution.
- Apply the file system recovery by the fsrepair command to the user LU file system failure (when any of the following SIM messages is output).
  - KAQK39500-E OS error Detail= 00 00 00 02 ,Level =00 , Type=02
  - KAQK39505-E OS error[cluster] Detail= 00 03 00 00 (01 03 00 00)

10.1.1 Types of fsrepair related commands

Table 10.1.1-1 shows the list of fsrepair related commands.

Table 10.1.1-1 List of fsrepair Related Commands

#	Command	Specification	Execution Example
1	ssh (node IP address)	ssh login	Troubleshooting “10.1.2.1 ssh login” (TRBL 10-0010)
2	fsrepair –L (file system name)	Recovery of failure file system (fsrepair command)	Troubleshooting “10.1.2.2 Recovery of failure file system” (TRBL 10-0010)

10.1.2 Execution method of fsrepair related commands

The execution method of fsrepair related commands is shown below.

The execution examples are described in the following assumptions.

Normal node : node0(D4Z7MNBX)
Failed node : node1
Failure file system name : LFS

Host name

Copyright © 2010, 2012, Hitachi, Ltd.

10.1.2.1 ssh login

The system administrator executes this command in the management console.
For executing the command in the management, log in to the node via ssh.

```
$ ssh nasroot@192.168.XX.XX
 Warning Notice!

 This is a {Company Name Here} computer system, which may be accessed and used only for authorized {Company Name
Here} business by authorized personnel. Unauthorized access or use of this computer system may subject violators to
criminal, civil, and/or administrative action.

 All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized
personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to
comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether
authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.
nasroot@D4Z7MNBX:~$
```

Figure 10.1.2.1-1 ssh Login window

10.1.2.2 Recovery of failure file system

The system administrator executes this command in the management console.
Execute the fsrepair command, and recover the file system from the blocked status.
Specify the file system name for the –L option.

```
nasroot@D4Z7MNBX:~$ sudo fsrepair -L LFS
```

Figure 10.1.2.2-1 Execution Example of the fsrepair Command

The execution examples are as shown below.

Copyright © 2010, 2012, Hitachi, Ltd.

```
nasroot@D4Z7MNBX:~$ sudo fsrepair -L LFS
Feb 11 02:25:22 Phase 1 - find and verify superblock...
Feb 11 02:25:22 Phase 2 - using internal log
Feb 11 02:25:22         - zero log...
Feb 11 02:25:22 ALERT: The filesystem has valuable metadata changes in a log which is being
Feb 11 02:25:22 destroyed because the -L option was used.
Feb 11 02:25:22         - scan filesystem freespace and inode maps...
Feb 11 02:25:22         - found root inode chunk
Feb 11 02:25:22 Phase 3 - for each AG...
Feb 11 02:25:22         - scan and clear agi unlinked lists...
Feb 11 02:25:22         - process known inodes and perform inode discovery...
Feb 11 02:25:22         - agno = 0
Feb 11 02:25:22         - agno = 1
Feb 11 02:25:22         - process newly discovered inodes...
Feb 11 02:25:22 Phase 4 - check for duplicate blocks...
Feb 11 02:25:22         - setting up duplicate extent list...
Feb 11 02:25:22         - check for inodes claiming duplicate blocks...
Feb 11 02:25:22         - agno = 0
Feb 11 02:25:22         - agno = 1
Feb 11 02:25:22 Phase 5 - rebuild AG headers and trees...
Feb 11 02:25:22         - reset superblock...
Feb 11 02:25:22 bogus quota flags 0x8000 set in superblock, bogus flags will be cleared
Feb 11 02:25:22 Phase 6 - check inode connectivity...
Feb 11 02:25:22         - resetting contents of realtime bitmap and summary inodes
Feb 11 02:25:22         - traversing filesystem ...
Feb 11 02:25:22         - traversal finished ...
Feb 11 02:25:22         - moving disconnected inodes to lost+found ...
Feb 11 02:25:22 Phase 7 - verify and correct link counts...
Feb 11 02:25:22 Note - quota info will be regenerated on next quota mount.
Feb 11 02:25:22 Phase 8 - check for quotas...
KAQG91304-I The file system is normal.
```

Figure 9.1.2.2-1 Example of Output Result of the fsrepair Command

After executing the fsrepair command, check whether the fsrepair command was executed correctly and the file system recovered.

If the result is terminated with the message “KAQG91304-I”, recovering the file system was successful. If the result is terminated with “KAQG91306-E”, recovering the file system failed.

Copyright © 2010, 2012, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2010, Hitachi, Ltd.

Chapter 11 Appendix B The Outline of the Troubleshooting Procedure

Figure 11-1 shows the outline of the overall flow on the whole troubleshooting chapter.

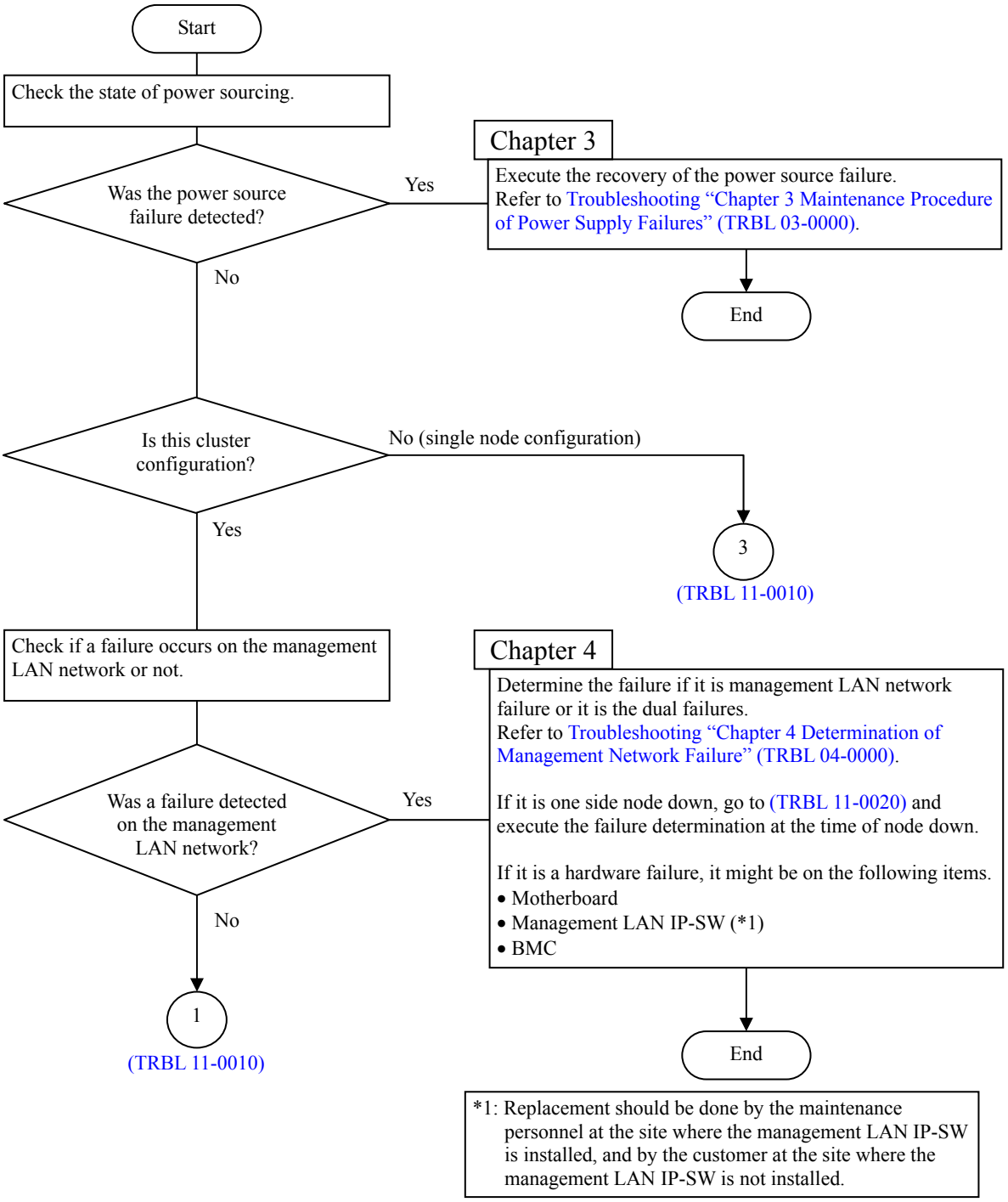


Figure 11-1 Troubleshooting Outline (1/4)

Copyright © 2010, 2014, Hitachi, Ltd.

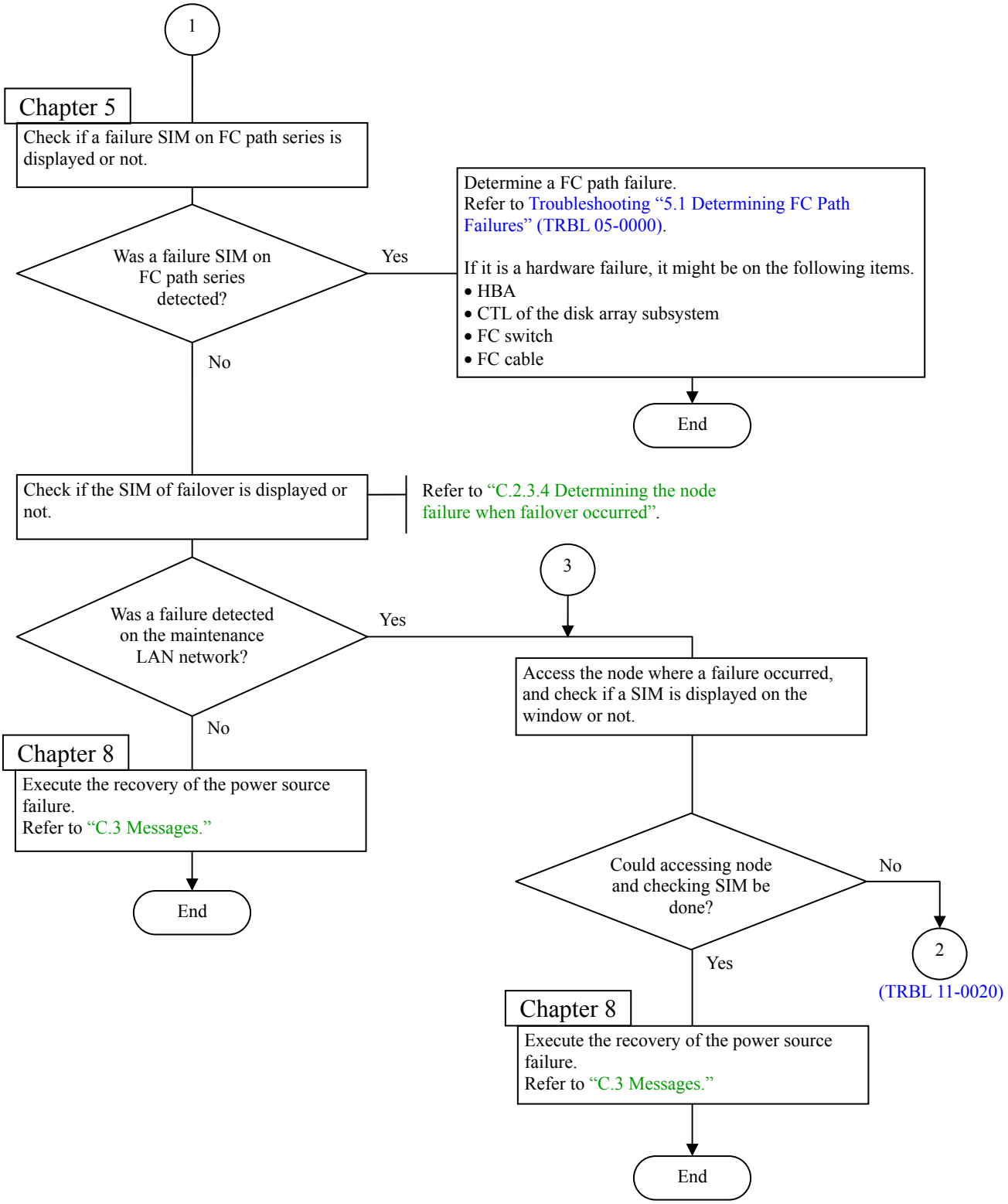
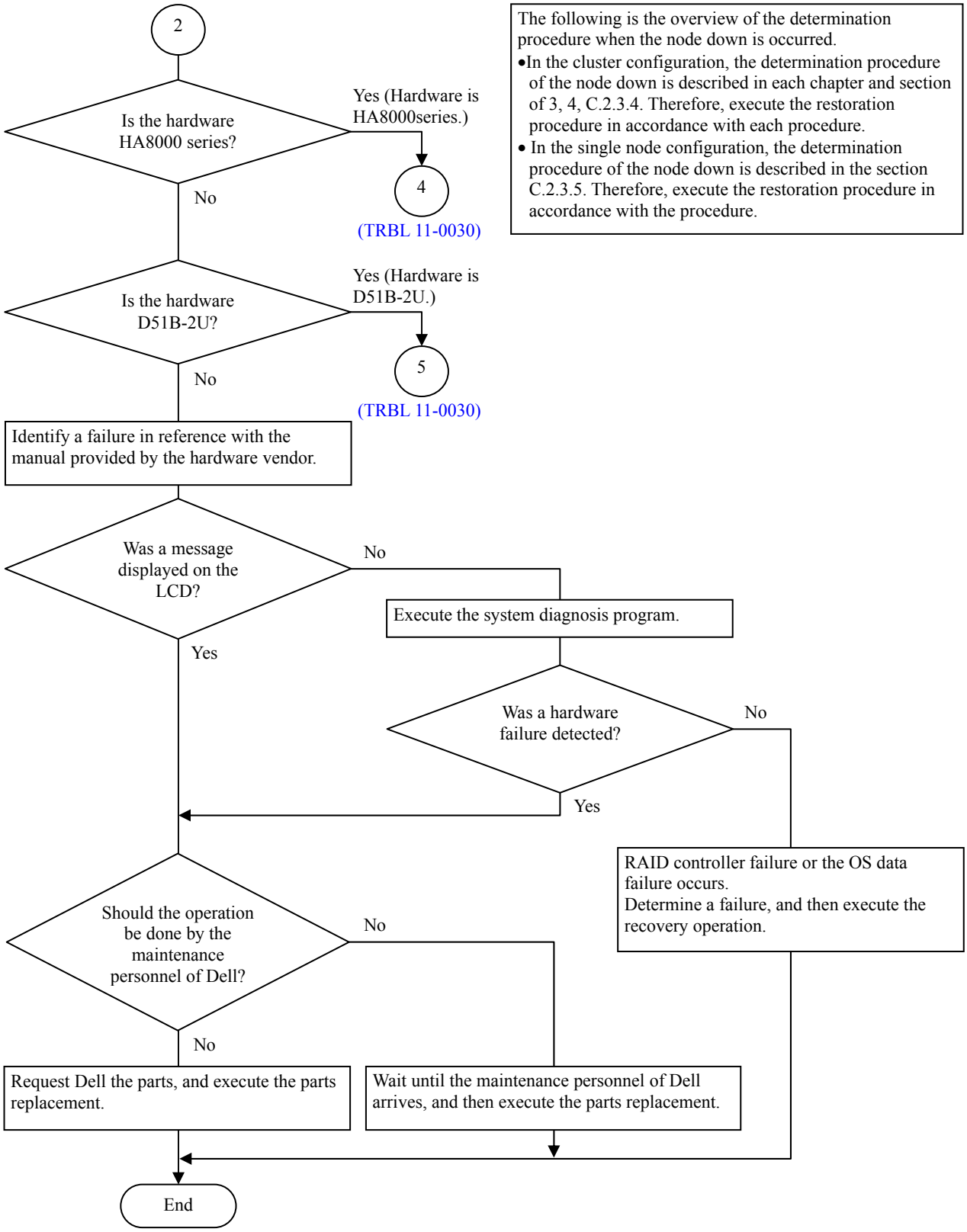


Figure 11-1 Troubleshooting Outline (2/4)

Copyright © 2010, 2014, Hitachi, Ltd.



The following is the overview of the determination procedure when the node down is occurred.

- In the cluster configuration, the determination procedure of the node down is described in each chapter and section of 3, 4, C.2.3.4. Therefore, execute the restoration procedure in accordance with each procedure.
- In the single node configuration, the determination procedure of the node down is described in the section C.2.3.5. Therefore, execute the restoration procedure in accordance with the procedure.

Figure 11-1 Troubleshooting Outline (3/4)

Copyright © 2010, 2015, Hitachi, Ltd.

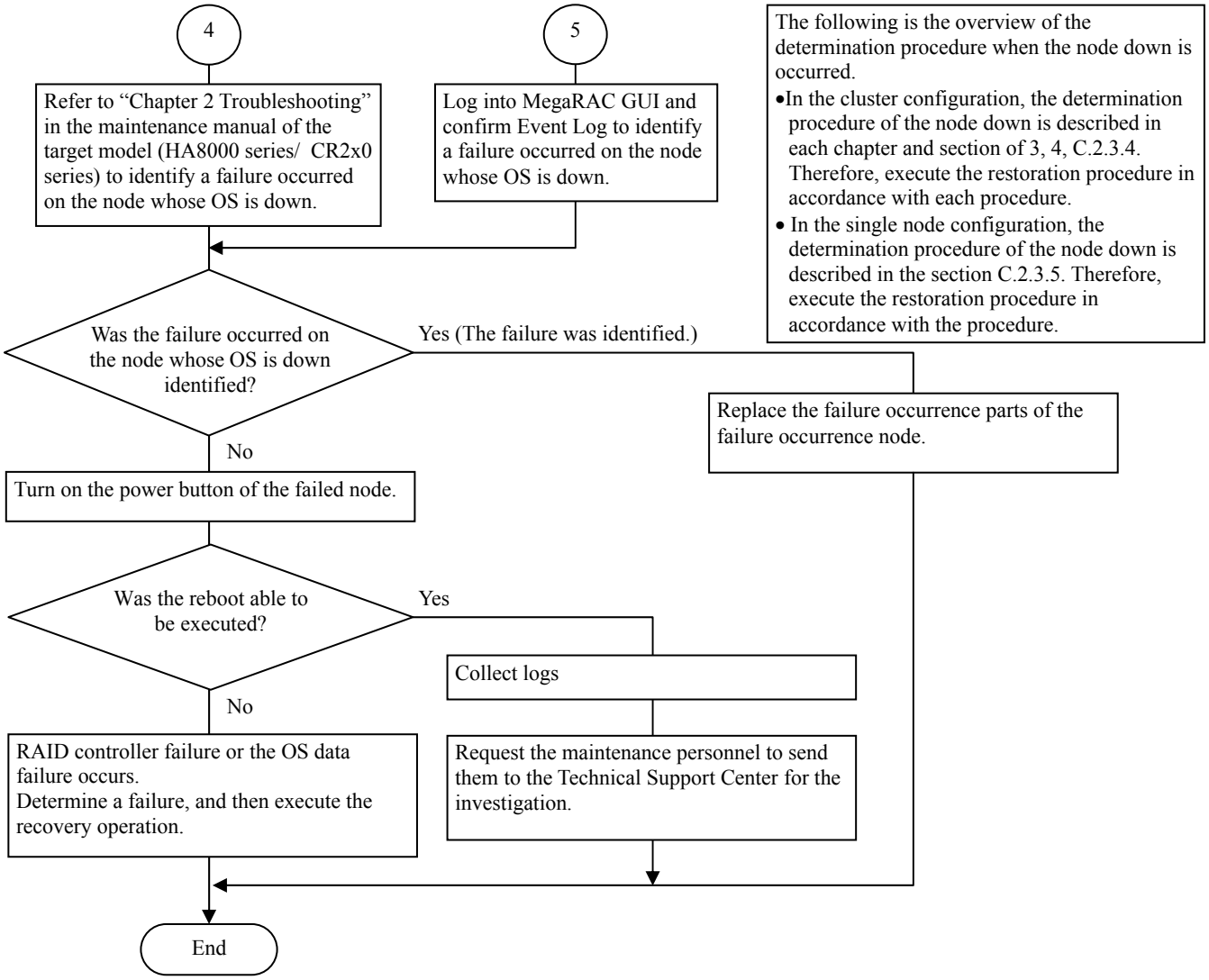


Figure 11-1 Troubleshooting Outline (4/4)

Copyright © 2010, 2015, Hitachi, Ltd.

Chapter 12 Appendix C The Entire Restoration Procedures on HDI Side in the Configuration of HDI for Cloud

In the configuration of HDI for Cloud, this section describes the procedures to restore the settings of entire systems from the initial statuses due to causes such as a disaster occurs on the HDI side.
Table 12-1 shows the summary of operation procedures and the operator to be operated. The details of procedures are expressed subsequently.
Ask the system administrator to select either of the following system setting information recovery procedures (after #6).

- When performing the recovery of the system setting information and the user data separately, perform the procedure with the check marks "✓" in the column "A".
- When performing the recovery of the system setting information and the user data from HCP collectively, perform the procedure with the check marks "✓" in the column "B" (check marks in brackets "(✓)" are performed by the procedures stated in the guide referred in #6-4).

Table 12-1 Summary of the Operation Procedures and the Operators

#	Selection		Operating Contents	Operator	Used Machine
	A	B			
1	✓	✓	Obtain the information which is required to be collected preliminarily	System administrator	Administration server (HSNM2)
2	✓	✓	Give the same serial number of the previous disk array subsystem to the newly shipped disk array subsystem	CTO operator	CTO operating PC (HSNM2)
				Maintenance personnel	Maintenance PC (HSNM2)
3	✓	✓	Reset the LU and port Information of disk array subsystem	CTO operator	CTO operating PC (HSNM2)
				Maintenance personnel	Maintenance PC (HSNM2)
4	✓	✓	Set up the Maintenance LAN IP-SW	CTO operator	CTO operating PC
				Maintenance personnel	Maintenance PC
5	✓	✓	(In the case of the cluster configuration, install on the both nodes) Newly install the OS on the node	CTO operator	KVM, Remote console CTO operating PC (CLI)
				Maintenance personnel	KVM, Maintenance PC (Remote console), Maintenance PC (CLI)
6	—	—	Restore the system setting information	—	—
6-1	✓		Request the administrator of HCP side to download the system setting information file from the HCP and transfer it to the HDI side.	HCP administrator	HCP administration server
6-2	✓		Upload the transferred system setting information file to the node	System administrator	Administration server (HFSM)
6-3	✓		Execute the system LU recovery	Maintenance personnel	Maintenance PC (CLI)
6-4		✓	Recover the system setting information and the user data from HCP collectively.	System administrator	Administration server (CLI)
7		(✓)	(In the case of the cluster configuration) Redefine the cluster	System administrator	Administration server (HFSM)
8	✓	(✓)	If the HCP payload encryption function is enabled, recover the encryption key.	System administrator	Administration server (CLI)
9	✓	(✓)	Start up the cluster and the resource group	System administrator	Administration server (HFSM)
10	✓		Forcibly stop the resource group	System administrator	Administration server (HFSM)
11	✓		Record the result of fslist	System administrator	Administration server (CLI)
12	✓		After deleting the file system, start the resource group and re-create the file system	System administrator	Administration server (HFSM)
13	✓		Execute the restoration of data in the file system	System administrator	Administration console (CLI)
14	✓		Set the sharing by using the information recorded in advance	System administrator	Administration server (HFSM)

☐ About the site of operation
#1 and #6 to #14 are done at the local site (at the customer site)
#2 to #5 is performed at CTO or local site (at the customer site) depending on the situation.

Copyright © 2010, 2011, Hitachi, Ltd.

12.1 Obtain the Information which is Required to be Collected Preliminarily

To execute the entire recovery process on the HDI side, it is assumed that the system administrator outputs the configuration information file of the disk array subsystem before occurrence of a failure and records the information at the time of creating the file system sharing.

Store the recorded information in the place unaffected failures of HDI side.

The following shows the method to get the necessary information that is required to collect beforehand.

For details, refer to “Hitachi Storage Navigator Modular2 Graphical User Interface (GUI) User’s Guide” and “User’s Guide ‘Managing File Shares’”.

12.1.1 Output the configuration information files of the RAID group and logical unit

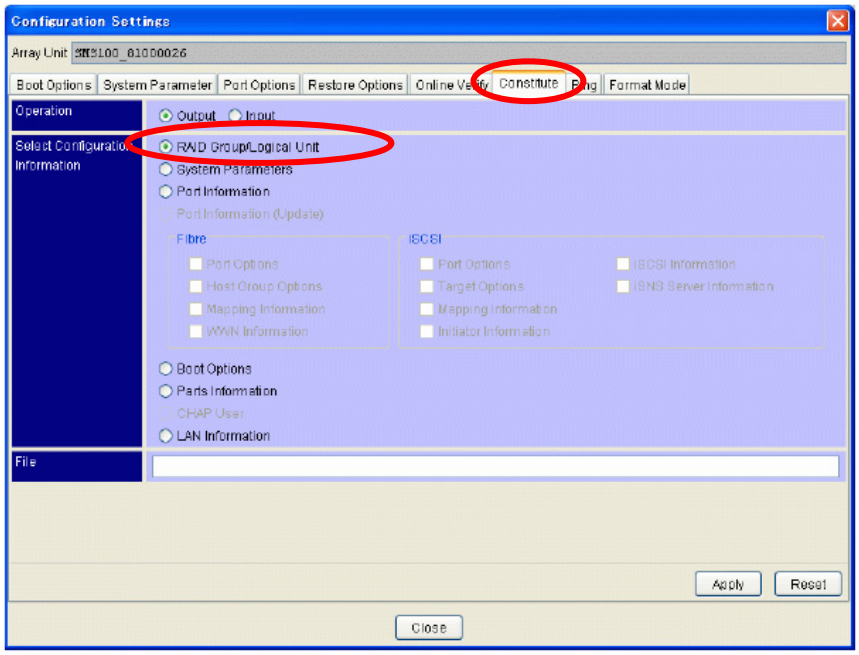


Figure 12.1.1-1 RAID Group/ Logical Unit Configuration Information File Output Screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click the radio button of [RAID Group/Logical Unit] at [Select Configuration Information].

(4) Specify a directory to be output the configuration information file and a file name to [File].
(e.g.): C:\work\RGInfo_20100514.txt
If you do not specify a directory, a file is created under the directory where the HSNM2 is installed.

(5) Click [Apply] button.

(6) The RAID group/ Logical unit information is output with the specified file name, and the confirmation message is displayed. Click [OK] button.

Copyright © 2010, 2011, Hitachi, Ltd.

The description above is an example when the target array is the AMS2000 series.

To output the configuration information files of the RAID group and the logical unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute procedure (1) to (8).

Note that the configuration information is obtained by selecting the “RAID Groups/DP Pools/Volumes” radio button.

Copyright © 2012, Hitachi, Ltd.

12.1.2 Output the configuration information file of a port information

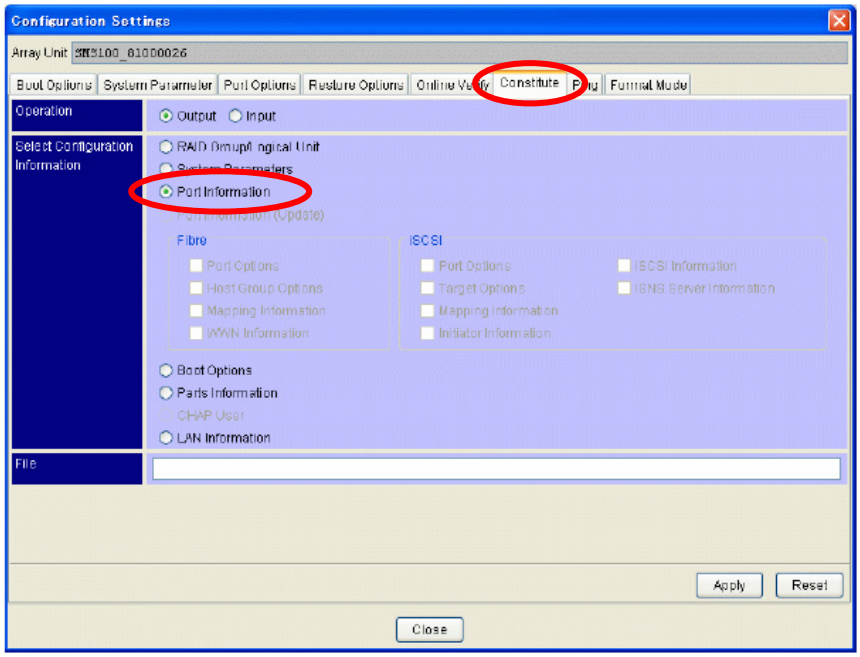


Figure 12.1.2-1 port information Configuration Information File Output screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click the radio button of [Port Information] at [Select Configuration Information].

(4) Specify a directory to be output the configuration information file and a file name to [File].
(e.g.): C:\work\port Info_20100514.txt
If you do not specify a directory, a file is created under the directory where the HSNM2 is installed.

(5) Click [Apply] button.

(6) The port information is output with the specified file name, and the confirmation message is displayed. Click [OK] button.

The description above is an example when the target array is the AMS2000 series.

To output the configuration information files of the RAID group and the logical unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute procedure (1) to (8).

Note that the configuration information is obtained by selecting the “Ports Information” radio button.

Copyright © 2010, 2012, Hitachi, Ltd.

12.1.3 Output the configuration information file of the system parameter

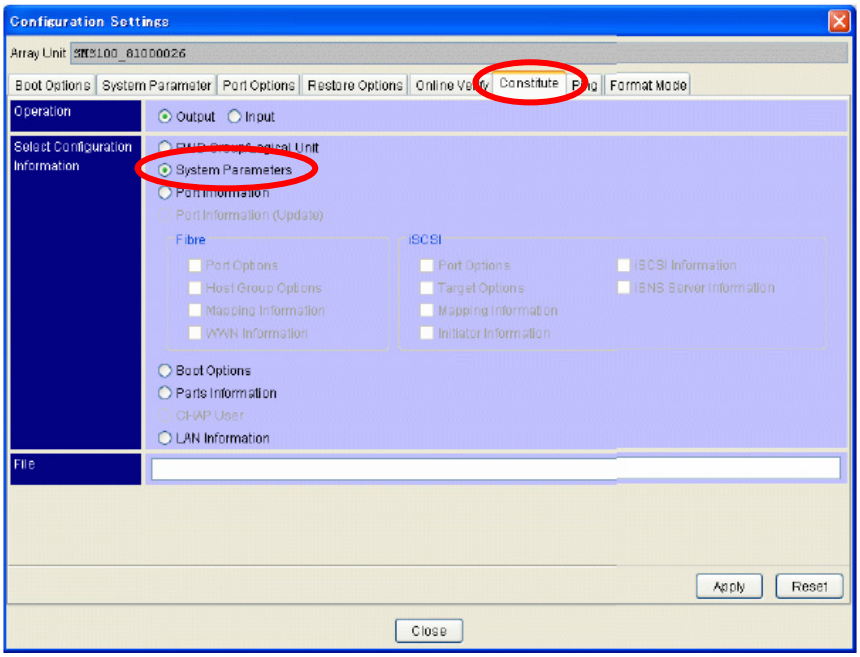


Figure 12.1.3-1 The configuration information file of the system parameter output screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click the radio button of [System Parameters] at [Select Configuration Information].

(4) Specify a directory to be output the configuration information file and a file name to [File].
(e.g.): C:\work\SystemParamInfo_20100514.txt
If you do not specify a directory, a file is created just under the directory where the HSNM2 is installed.

(5) Click [Apply] button.

(6) The port information is output with the specified file name, and the confirmation message is displayed. Click [OK] button.

The description above is an example when the target array is the AMS2000 series.

To output the configuration information files of the RAID group and logical unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute procedure (1) to (8).

Note that the configuration information is obtained by selecting the “System Parameters” radio button.

Copyright © 2010, 2012, Hitachi, Ltd.

12.1.4 Record the shared setting of file system

Use nfsbackup and cifsbackup command, and obtain the backup of the common information.

For the reference place in User's Guide describing the details about nfsbackup command, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 6 'nfsbackup" (GENE 00-0060)", and for the reference place in User's Guide describing the details about cifsbackup command, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 6 'cifsbackup" (GENE 00-0060)".

NOTE: If the both CIFS sharing and NFS sharing are set for a file system, execute the both of cifsbackup and nfsbackup command.

CIFS sharing uses cifsbackup command. The following shows an example.

- The file system name is "fs01".
- The information definition file name to be output is "fs01_cifsshares.xml".

```
$ sudo cifsbackup fs01 fs01_cifsshares.xml
```

Figure 12.1.4-1 An example of cifsbackup command execution

NFS sharing uses nfsbackup command. The following shows an example.

- The file system name is "fs01".
- The information definition file name to be output is "fs01_nfsshares.xml".

```
$ sudo nfsbackup fs01 fs01_nfsshares.xml
```

Figure 12.1.4-2 An example of nfsbackup command execution

The acquired contents of information definition file can be referred by the cifsrestore command and nfsrestore command.

The form of command is such as follows.

- cifsrestore --list <Information definition file name>
- nfsrestore --list <information definition file name>

When there is no backup file, it is required to input the information that is necessary to create "share" manually and to set the sharing again. When there is no backup file, and no information to input manually, the sharing cannot be set again.

In the case you will input them manually, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Adding a file share" (GENE 00-0050)" for the reference place in User's Guide, and record the information described in Figure 12.1.4-1 to Figure 12.1.4-6.

Table 12.1.4-1 Information to be specified at [Basic] tab on the [Add Share] dialog

#	Items to be set	Setting contents
1	Sub-directory name	
2	Protocol	
3	Export point owner	

Copyright © 2010, 2012, Hitachi, Ltd.

Table 12.1.4-2 Information to be specified at [CIFS] sub-tab of [Access Control] tab on the [Add Share] dialog

#	Items to be set	Setting contents
1	Enable ACL	
2	Read only	
3	Special permitted users/groups	
4	Host/network based access restriction	
5	Browsable share	
6	Allow guest account access	
7	Access permissions for new files	
8	Access permissions for new directories	

Table 12.1.4-3 Information to be specified at [NFS] sub-tab of [Access Control] tab on the [Add Share] dialog

#	Items to be set	Setting contents
1	Host/network	
2	Security flavor	
3	Anonymous mapping	
4	UID for anonymous mapping	
5	GID for anonymous mapping	

Table 12.1.4-4 Information to be specified at [Directory] sub-tab of [Access Control] tab on the [Add Share] dialog in the case of Advanced ACL type

#	Items to be set	Setting contents
1	User or group name	
2	Permissions	
3	Apply these ACLs to this folder, sub- folders, and files	

Table 12.1.4-5 Information to be specified at [Directory] sub-tab of [Access Control] tab on the [Add Share] dialog in the case of Classic ACL type

#	Items to be set	Setting contents
1	Export point permissions	
2	Unix sticky bit	

Table 12.1.4-6 Information to be specified at [CIFS] sub-tab of [Advanced] tab on the [Add Share] dialog

#	Items to be set	Setting contents
1	CIFS share name	
2	Comment shown to CIFS clients	
3	Enable auto creation of home directory	
4	Users allowed to change file time stamp	
5	Disk synchronization policy	
6	Windows(R) client access policy	
7	Allow CIFS client cache	
8	Use Volume Shadow Copy Service	

Copyright © 2010, Hitachi, Ltd.

12.1.5 Record the name space name of the HCP to be connected

To use the information stored in the HCP at the time of failure recovery, it is required to record the name space name of HCP to be connected per file system.
Record the name space name of HCP to be connected when the migration policy is set to the file system, or confirm it on the screen of HFSM.

When confirming the name space name of HCP to be connected on the screen of HFSM, open the Figure12.1.5-1 "[3.Source/Target] window in the Migration Wizard", ①select the file system name from [File System Name] pull down menu, and ②check the name space name to be displayed on the [Namespace name:].
After checking the name spaces for all of the file systems, ③click [Cancel] button to terminate Migration Wizard.

For the reference place in User's Guide describing the details about the operation method of Migration Wizard, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Setting migration policies'' (GENE 00-0050)".

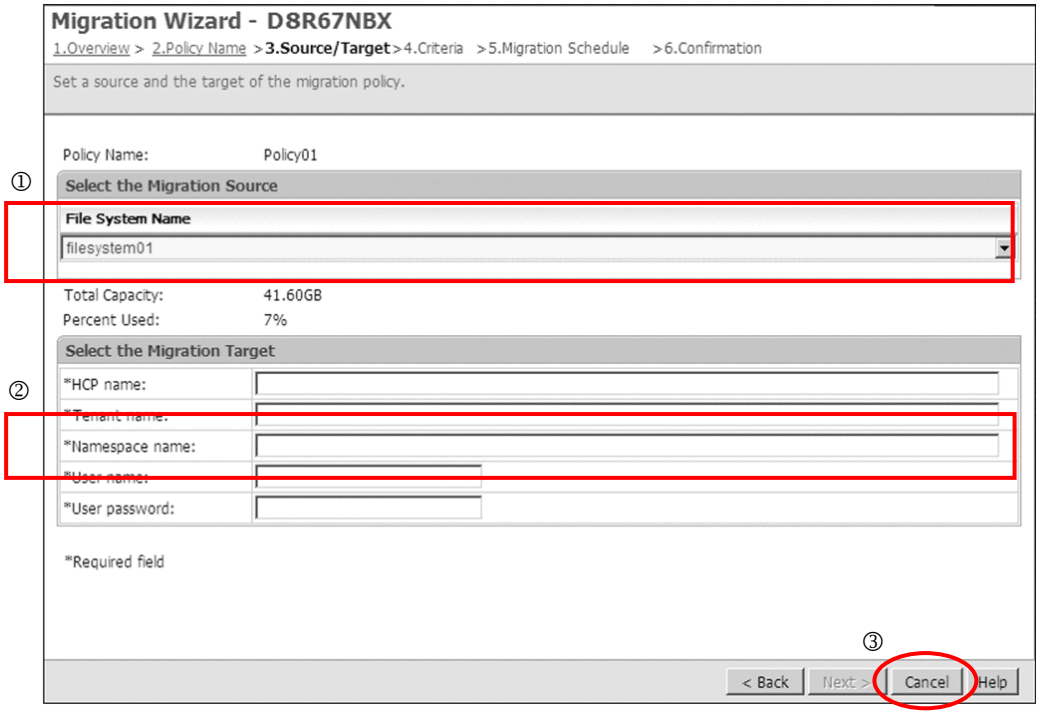


Figure 12.1.5-1 [3.Source/Target] window in the Migration Wizard

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the "User's Guide" for the version.

Perform 12.1.4 and 12.1.5, and record the information of CIFS sharing and NFS sharing and the name space name of HCP per file system as described in the Figure 12.1.5-2.

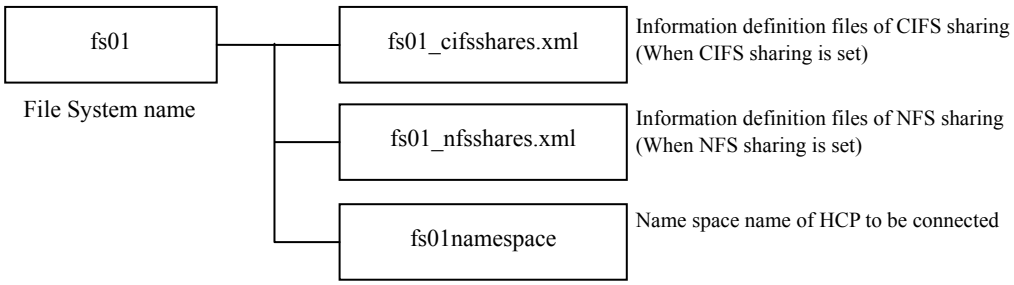


Figure12.1.5-2 Information to be obtained per file system

Copyright © 2010, 2012, Hitachi, Ltd

12.1.6 Prepare the Password and the Passphrase of the HCP Payload Encryption Function

If the HCP payload encryption function is used in the OS version 5.2.0-XX or later, the password and passphrase are required to use the data stored in HCP.

Notify the system administrator to prepare the password and the passphrase before starting the data recovery procedure.

Copyright © 2015, Hitachi, Ltd

12.2 Give the Same Operating Serial Number of the Previous Disk Array Subsystem to the Newly Shipped Disk Array Subsystem

Obtain the serial number of the disk array subsystem where a failure occurs from the distributor.

(It is assumed that the distributor controls the serial numbers of the disk array subsystems.)

Register the obtained serial number to the disk array subsystem to be shipped newly.

12.2.1 How to register the operating serial number of the disk array subsystem

Change the serial number of the disk array subsystem by using the operating serial number setup function from the WEB browser of disk array subsystem.

The procedures are described below.

(1) Shift the disk array subsystem to maintenance mode.
Press RST SW of Controller #0. The ALARM LED (red) of the controller #0 turns on.
After turning on the ALARM LED (red) of the controller #0, press RST SW of controller #1 within 10 seconds.
ALARM LED (red) of controller #0 turns off, READY LED (green) of the front bezel turns off, and it shift to the maintenance mode.
If it does not shift to the maintenance mode, refer to “WEB Chapter 3. The Maintenance Mode Operation Procedure” in each maintenance manual.

(2) Input the “http:// IP address of disk array subsystem/equip_set” in the address bar of WEB browser.
[User name] or [Password] may be requested in the operation of WEB connection or WEB operation.
In that case, input the user name “maintenance” and the password “hosyu9500”.

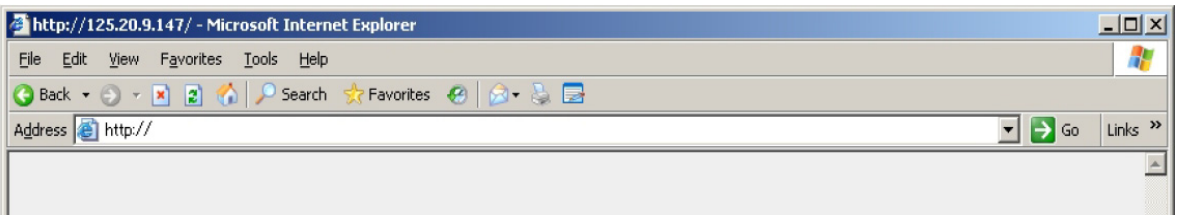


Figure 12.2.1-1 Address input bar of the browser

Copyright © 2010, 2012, Hitachi, Ltd.

(3) Figure 12.2.1-2 Equipment Information Setup screen is displayed.
Click [Change] button.

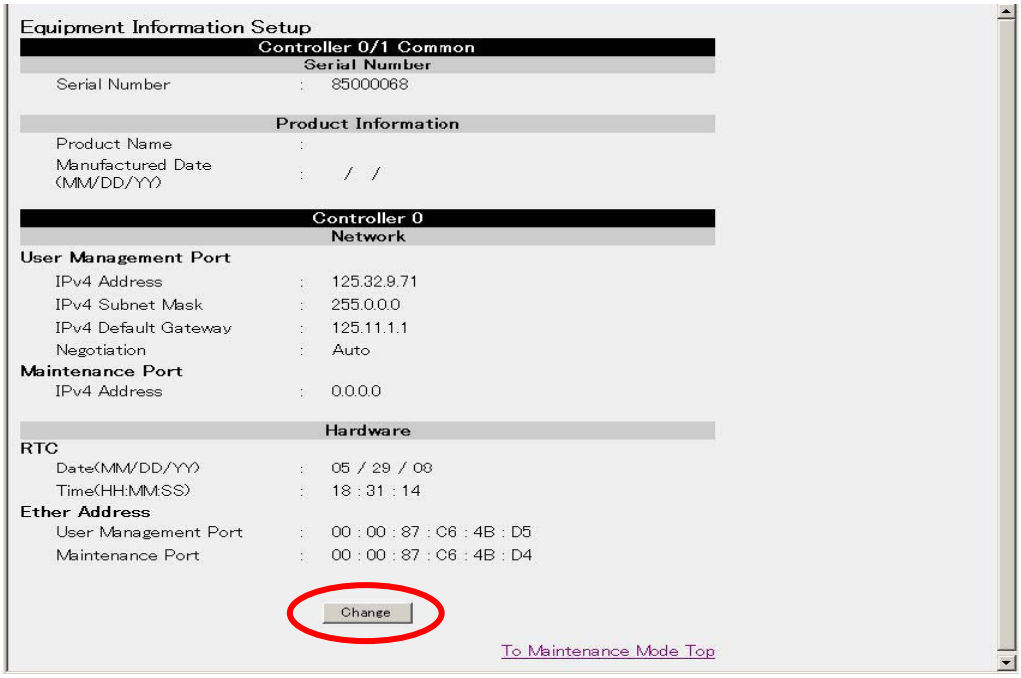


Figure 12.2.1-2 Equipment Information Setup screen (1)

(4) In [Serial Number], input the serial number obtained from the distributor before the failure occurrence, and then click [Set] button.

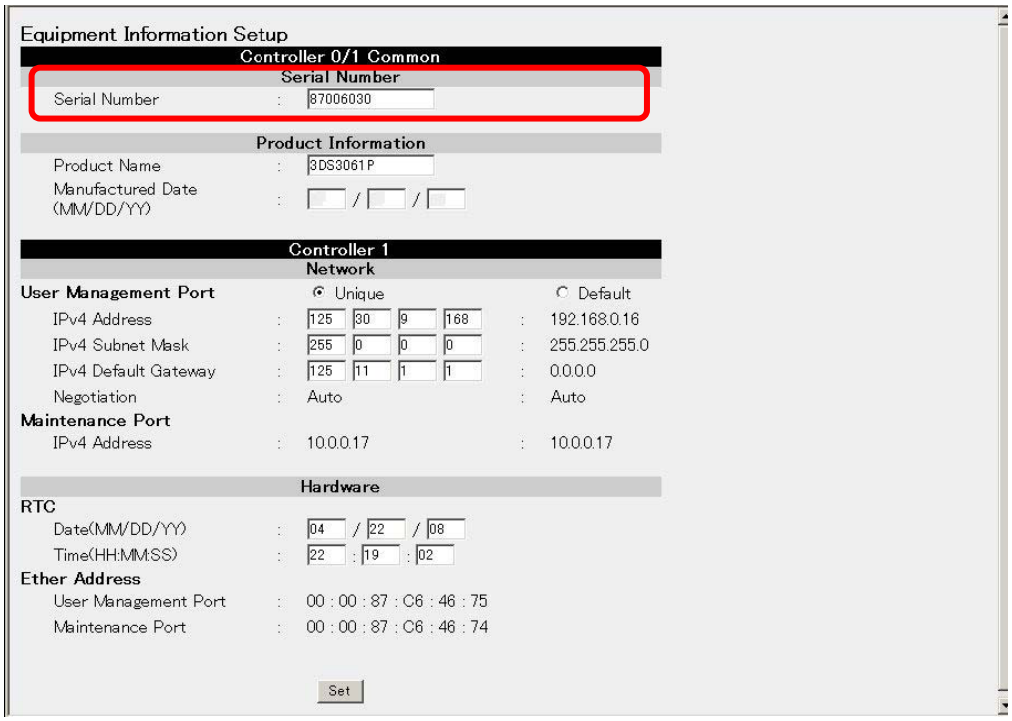


Figure 12.2.1-3 Equipment Information Setup screen (2)

Copyright © 2010, Hitachi, Ltd.

(5) Check that there is no error in the changed contents, and then click [Save] button.
Complete screen is displayed and the serial number is changed.

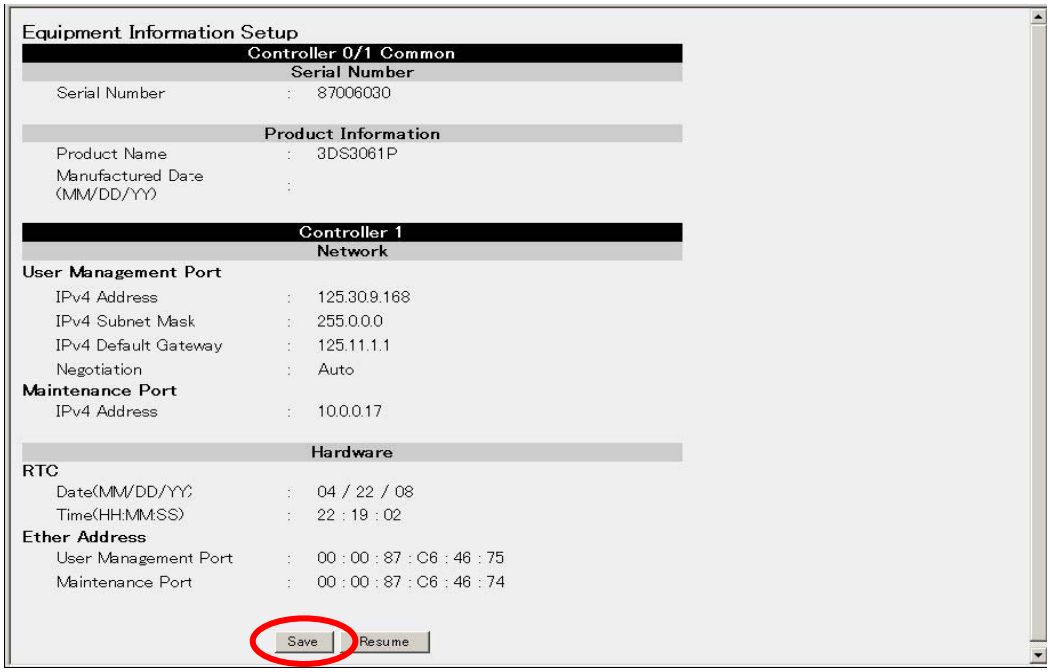


Figure 12.2.1-4 Equipment Information Setup screen (3)

(6) Input the "http://IP address of disk array subsystem/" in the address bar of WEB browser.
It shows the web screen of figure 12.2.1-5 Disk array subsystem.

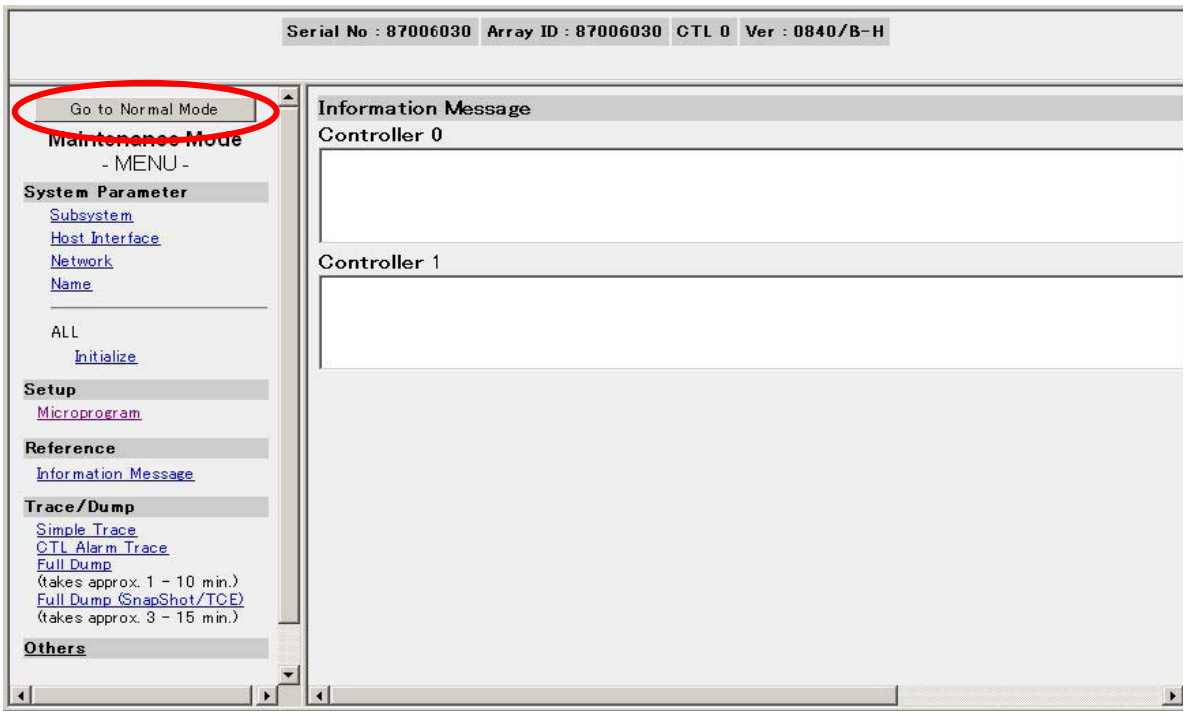


Figure 12.2.1-5 Disk array subsystem Web screen

Copyright © 2010, Hitachi, Ltd.

(7) Click [Go To Normal Mode] button on the web screen of Figure 12.2.1-5 Disk Array Subsystem. Figure 12.2.1-6 restart confirmation dialog is displayed. Click [OK] button.

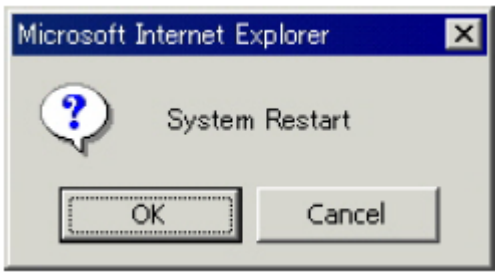


Figure 12.2.1-6 Restart Confirmation Dialog

(8) Figure 12.2.1-7 Reboot executing screen is displayed.

Figure 12.2.1-7 Reboot Executing screen

(9) Disk array subsystem becomes READY status in 5 to 15 minutes.
Check that the READY LED (green) of the disk array subsystem is on, and then terminate the WEB screen.

Copyright © 2010, Hitachi, Ltd.

12.3 Reset the LU and Port Information of Disk Array Subsystem

Restore the setting of disk array subsystem with the collected information at the process of Troubleshooting "12.1 Obtain the Information which is Required to Collect Preliminarily" (TRBL 12-0010).

For details, refer to "Hitachi Storage Navigator Modular2 Graphical User Interface (for GUI) User's Guide".

12.3.1 Restore the setting from the configuration information file where the RAID group/ Logical Unit is obtained

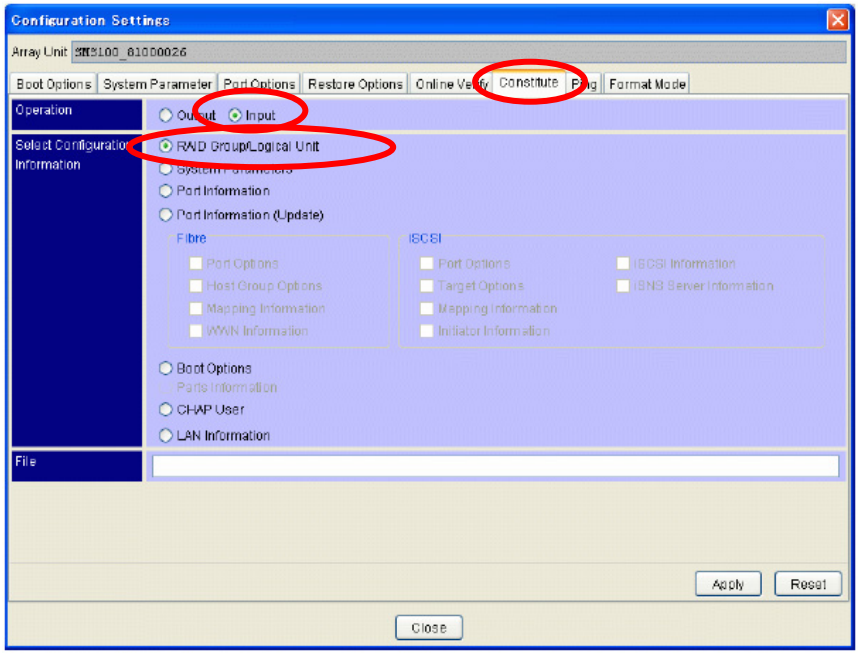


Figure 12.3.1-1 RAID group/ Logical Unit Configuration information file Input Screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click [Input] radio button at [Operation].

(4) Click [RAID Group/Logical Unit] radio button at [Select Configuration Information].

(5) Specify the RAID group definition, the directory of the file that is described the group definition and logical unit definition, and its file name in [File].
(e.g.): C:\work\RGInfo_20100514.txt

(6) Click [Apply] button.

(7) The confirmation message is displayed. Then click [OK] button.

Copyright © 2010, Hitachi, Ltd.

The description above is an example when the target array is the AMS2000 series.

To restore the setting from the configuration information file of the RAID group/ Logical Unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute (9) and the rest of the procedures to restore the setting by using the configuration information file obtained from Troubleshooting “12.1.1 Output the configuration information files of the RAID group and logical unit” (TRBL 12-0010).

Copyright © 2012, Hitachi, Ltd.

12.3.2 Restore the Port Information setting from the configuration information file

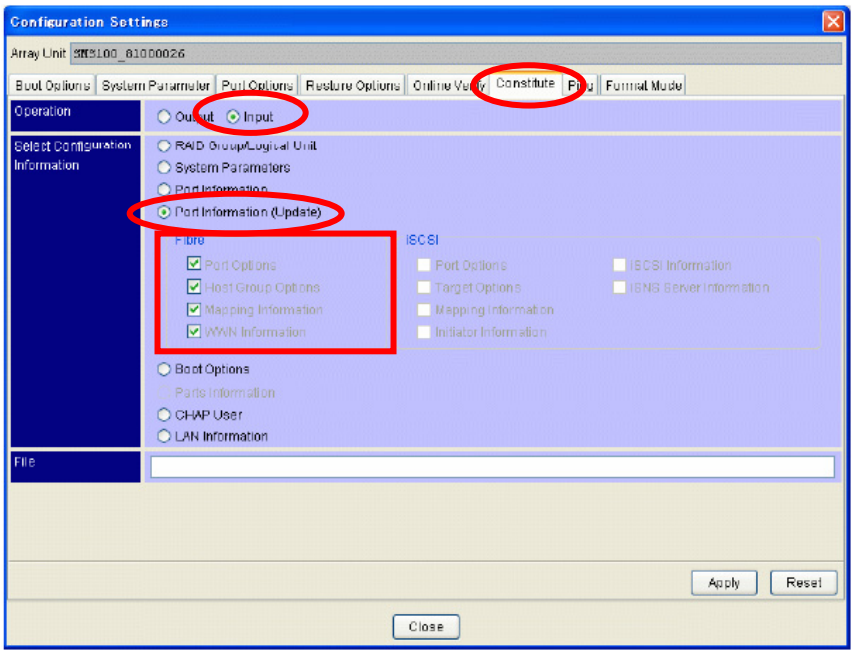


Figure 12.3.2-1 Port Information Configuration Information File Input Screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click [Input] radio button at [Operation].

(4) Click [RAID Group/Logical Unit] radio button at [Select Configuration Information].

(5) Select all of the check boxes in the Fibre group under [Port Information (Update)].
An error occurs if no item is selected.

(6) Specify the directory where port information is input and its file name in [File].
(e.g.): C:\work\PortInfo_20100514.txt

(7) Click [Apply] button.

(8) The port information is input with the specified file name, and the confirmation message is displayed. Then click [OK] button.

(9) If customer used LUN Manager function on AMS, node WWN information settings on AMS should be changed, because the node has been new one. To obtain new node WWN, refer to "Disk Setting '2.3 Acquiring WWNs of Nodes'(DSKST 02-0090)".
To set the LUN Manager, refer to "Hitachi Storage Navigator Modular2 Graphical User Interface(for GUI) User's Guide".

Copyright © 2010, Hitachi, Ltd.

The description above is an example when the target array is the AMS2000 series.

To restore the setting from the configuration information file of the RAID group/ Logical Unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute (9) and the rest of the procedures to restore the setting by using the configuration information file obtained from Troubleshooting “12.1.2 Output the configuration information file of a port information” (TRBL 12-0020).

Copyright © 2012, Hitachi, Ltd.

12.3.3 Restore the setting from the configuration information file where the system parameter is obtained

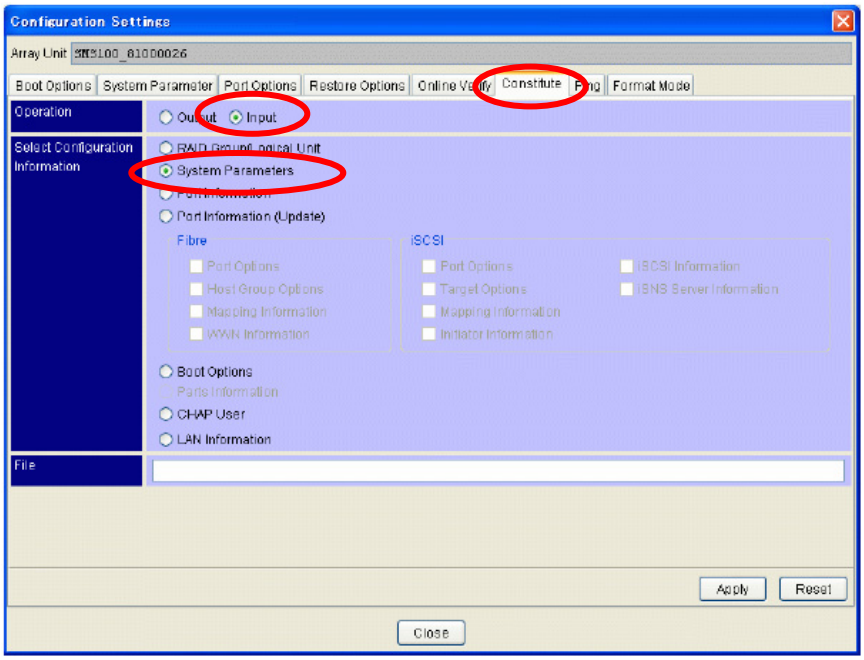


Figure 12.3.3-1 System Parameter Configuration Information File Output Screen

(1) Select the configuration setting from the tool menu on the unit screen.

(2) Click [Constitute] tab.

(3) Click [Input] radio button at [Operation].

(4) Click the radio button of system parameter at [Select Configuration Information].

(5) Specify the directory of the file that is described the system parameter and its file name in the [File].
(e.g.): C:\work\SystemParamInfo_20100514.txt

(6) Click [Apply] button.

(7) The confirmation message is displayed. Then click [OK] button.

The description above is an example when the target array is the AMS2000 series.

To restore the setting from the configuration information file of the RAID group/ Logical Unit when the target array is the HUS100 series, refer to “System Parameter ‘Chapter 10. Setting Constitute Array’” in the maintenance manual and execute (9) and the rest of the procedures to restore the setting by using the configuration information file obtained from Troubleshooting “12.1.3 Output the configuration information file of the system parameter” (TRBL 12-0030).

Copyright © 2010, 2012, Hitachi, Ltd.

12.4 Set Up the Maintenance LAN IP-SW

At the site where the Management LAN IP-SW is installed, execute the setting of LAN IP-SW.

For details, refer to Hitachi Data Ingestor Maintenance Manual "Installation 'Chapter 4 Overview of VLAN Setting Procedure for the Management LAN IP-SW' (INST 04-0000)".

At the site where no Management LAN IP-SW is installed, request the customer to set the IP-SW provided by the customer.

Copyright © 2010, 2011, Hitachi, Ltd.

12.5 Newly Install the OS on the Node

To execute the restoration of system LU, install the OS newly on the node.

The following shows the overview of the newly installation.

For the procedure of the newly installation, refer to "Set Up 'Chapter 3 New Installation' (SETUP 03-0000)".

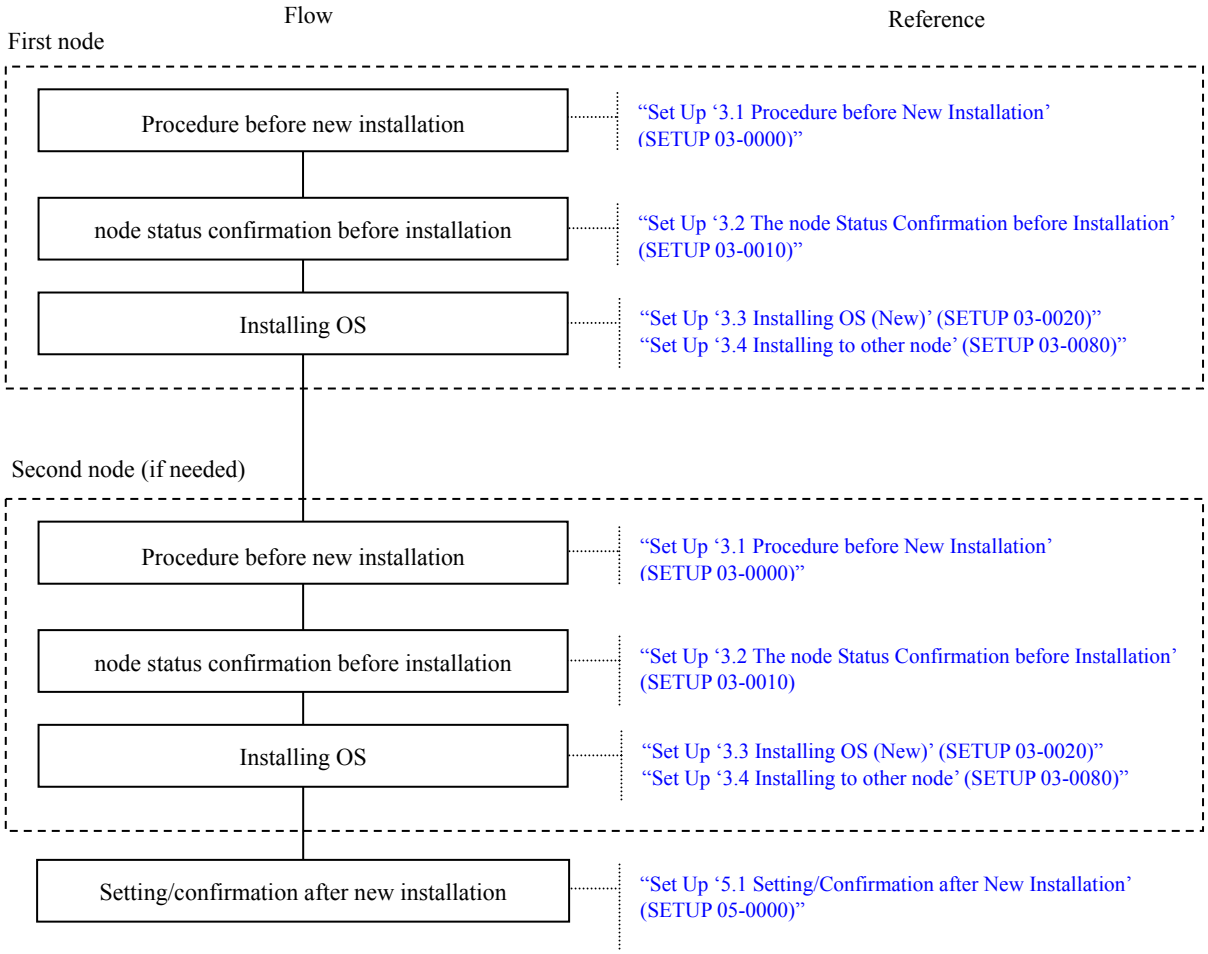


Figure 12.5-1 Flow of New Installation Procedure

Copyright © 2010, 2015, Hitachi, Ltd.

12.6 Restore System Setting Information File

Ask the system administrator to select either of the following restore methods of the system setting information.

To restore the system setting information separately from the user data using the downloaded system setting information file, perform the procedure 12.6.1 (Pattern “A” in Table 12-1).

To restore the recovery of the system setting information and the user data from HCP collectively, perform the procedure 12.6.2 (Pattern “B” in Table 12-1).

12.6.1 Restore the Downloaded System Setting Information File

12.6.1.1 Request the Administrator of HCP Side to Download the System Setting Information File from the HCP and Transfer It to the HDI Side

To execute the restoration of system LU, it is required to obtain the system setting information file that is already transferred to HCP side.

Report the name space name of the target HCP to be connected, which is obtained at the process of Troubleshooting “12.1.5 Record the name space name of the HCP to be connected” (TRBL 12-0060) to the administrator on the HCP side, and then request the administrator to transfer the system setting information file to the side of HDI, after downloading it from the HCP.

File transferring should be done by such as an e-mail or FTP which can be executed the file transferring.

Copyright © 2010, 2015, Hitachi, Ltd.

12.6.1.2 Upload the Transferred System Setting Information File to the Node

Register the node information to be connected into HFSM and Upload the system setting information file that is transferred from the HCP administrator to the node.

For the reference place in User's Guide describing the details about registering node information to be connected into HFSM, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Registering a processing node" (GENE 00-0040)".
For the reference place in User's Guide describing the details about uploading a system configuration file, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Uploading a system configuration file" (GENE 00-0050)".

The following shows the procedures to upload the system setting information file.

This operation is available to do from [<Physical Node>] sub window.

(1) Click [Save Settings] button in [Settings] tab.
[Save System Settings Menu] page of [Save Settings] dialog is displayed.

(2) Click [Upload Saved Data] button.
[Upload Saved Data] page shown in the Figure 12.6.1-1 is displayed.

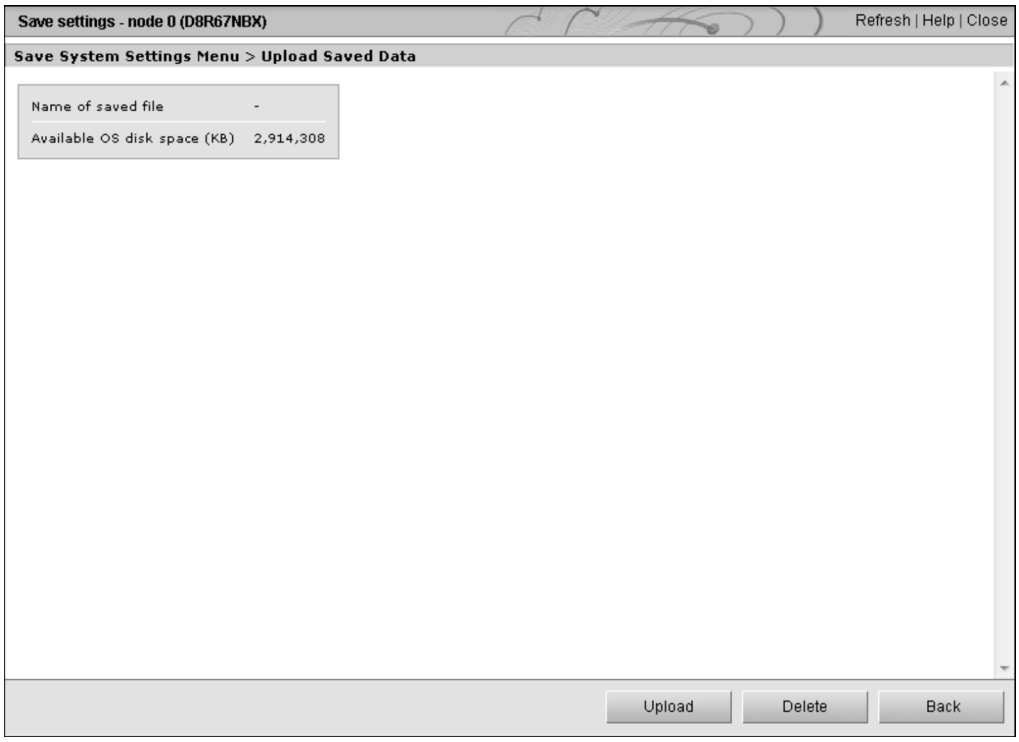


Figure 12.6.1-1 [Upload Saved Data] Page

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the "User's Guide" for the version.

Copyright © 2010, 2015, Hitachi, Ltd.

(3) Check the information displayed in the screen, and click [Upload] button.
[Select Saved Data File] page is displayed.

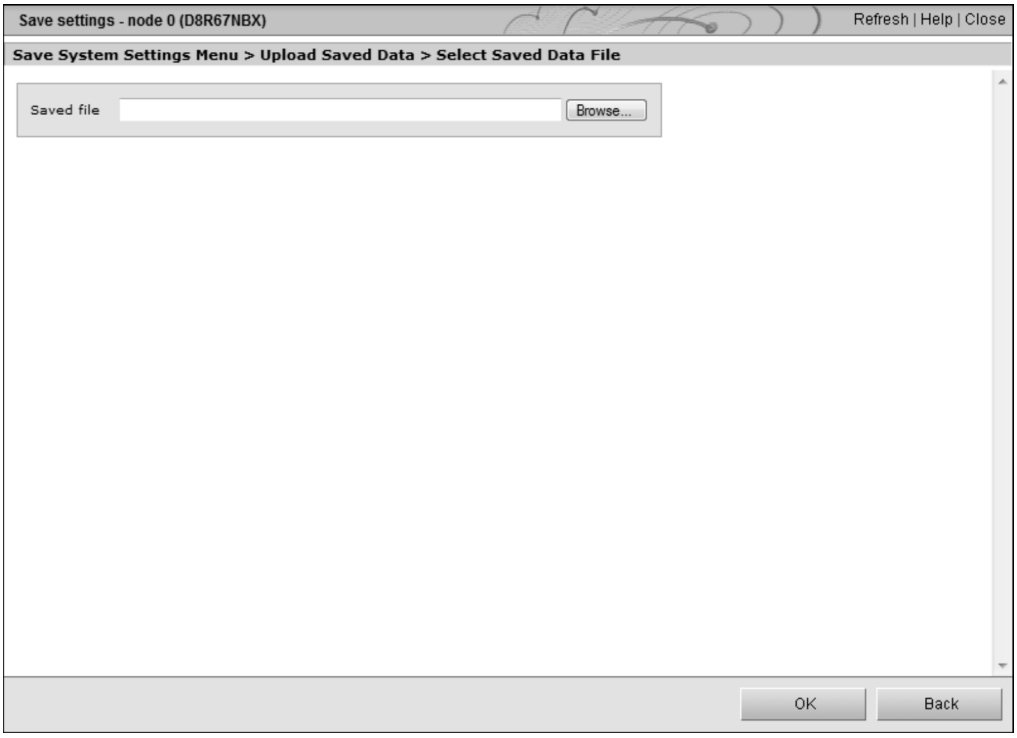


Figure 12.6.1-2 [Select Saved Data File] page

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the "User's Guide" for the version.

(4) Specify the path of system setting information file to be uploaded to [Saved file] with the absolute path. Click [Browse] button when you refer the file name to specify it, click [Browse] button.

(5) Click [OK] button.
The system setting information file is uploaded, and the screen returns to [Upload Saved Data] page. The information of the uploaded system setting information file is displayed.

Copyright © 2010, 2015, Hitachi, Ltd.

12.6.1.3 Execute the System LU Recovery

Execute the restoration process of the system LU. For details, refer to "Maintenance Tool '2.8.2 (1) Batch Recovery of the OS Disk/cluster management LU' (MNTT 02-0470)".

The following shows the execution procedures of the System LU restoration.

Execute syslurestore command, and restore the system LU.

The execution confirmation message is displayed at the time of command execution. Input "y" to continue the process.

```
$ sudo syslurestore -f sysbk_FC-GW6P67NBX_20100111_0352.tgz
KAQM13133-Q Processing might take a while. Do you want to restore the settings for the cluster
management LU and both of the OS disks in the cluster by using the saved file (saved date and time =
2010/01/11 03:52)? (y/n)
```

Figure 12.6.1-3 An Example of System LU Restoration Command Execution

Copyright © 2010, 2015, Hitachi, Ltd.

12.6.2 Recover the System Setting Information and the User Data Collectively using the HCP Linkage Function

Recover the system setting information and the user data collectively. When the recovery is complete, the OS reboots.

For the detailed procedure, refer to “Restoring system configuration information and user data in batch” in “Troubleshooting Guide”.

Perform the cluster redefinition, recovery of the encryption key and start of the cluster/resource group in the command dialogues or the procedure in the reference guide. For the password and the passphrase required to enter during the command dialogue, use the password and the passphrase prepared in Troubleshooting “12.1.6 Prepare the Password and the Passphrase of the HCP Payload Encryption Function” (TRBL 12-0061).

```
$ sudo syslurestore --trans --system-name cluster01
[Transfer settings]
host-name: hcap.hitachi.com
host-address: 10.208.21.100
tenant-name: tenant
user-name: user
password:

(Snip)

KAQM13185-Q Processing might take about 120 seconds. Do you want to restore system settings by using the saved file? (y/n) y
Restoring the system configuration. (remaining time = 120 seconds)
  Step 1/9 Performing pre-processing.  (remaining time = 120 seconds)
  Step 2/9 Decompressing the system backup files. (remaining time = 120 seconds)
  Step 3/9 Initializing management area-1. (remaining time = 110 seconds)
  Step 4/9 Initializing management area-2. (remaining time = 100 seconds)
  Step 5/9 Initializing management area-3. (remaining time = 90 seconds)
  Step 6/9 Restoring the system files. (remaining time = 80 seconds)
  Step 7/9 Creating the file systems. (remaining time = 70 seconds)
  Step 8/9 Restoring the file systems. (remaining time = 60 seconds)
      1/4 Filesystem01 (remaining time = 50 seconds)
      2/4 Filesystem02 (remaining time = 40 seconds)
      3/4 Filesystem03 (remaining time = 30 seconds)
      4/4 Filesystem04 (remaining time = 20 seconds)
  Step 9/9 Performing post-processing. (remaining time = 10 seconds)
KAQM13171-I The settings for the cluster management LU and the OS disk have been restored, and the OS has been restarted.
```

Figure 12.6.2-1 Example of System Collective Recovery Command

Copyright © 2015, Hitachi, Ltd.

12.7 Redefine the Cluster

NOTE: If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not necessary because it is performed in the reference guide stated in 12.6.2.

After executing the system LU restoration, the cluster configuration is required to redefine.

For the reference place in User's Guide describing the details about defining a cluster configuration, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Defining a cluster configuration" (GENE 00-0040)".

The following shows the procedures to redefine the culuster configuration.

(1) Click [Cluster Management] button in [Settings] tab.
[Define Cluster Configuration] page in [Cluster Management] dialog is displayed, and the message dialog that urges to define the cluster configuration is displayed.

(2) Click [OK] button.
[Define Cluster Configuration] page is displayed.

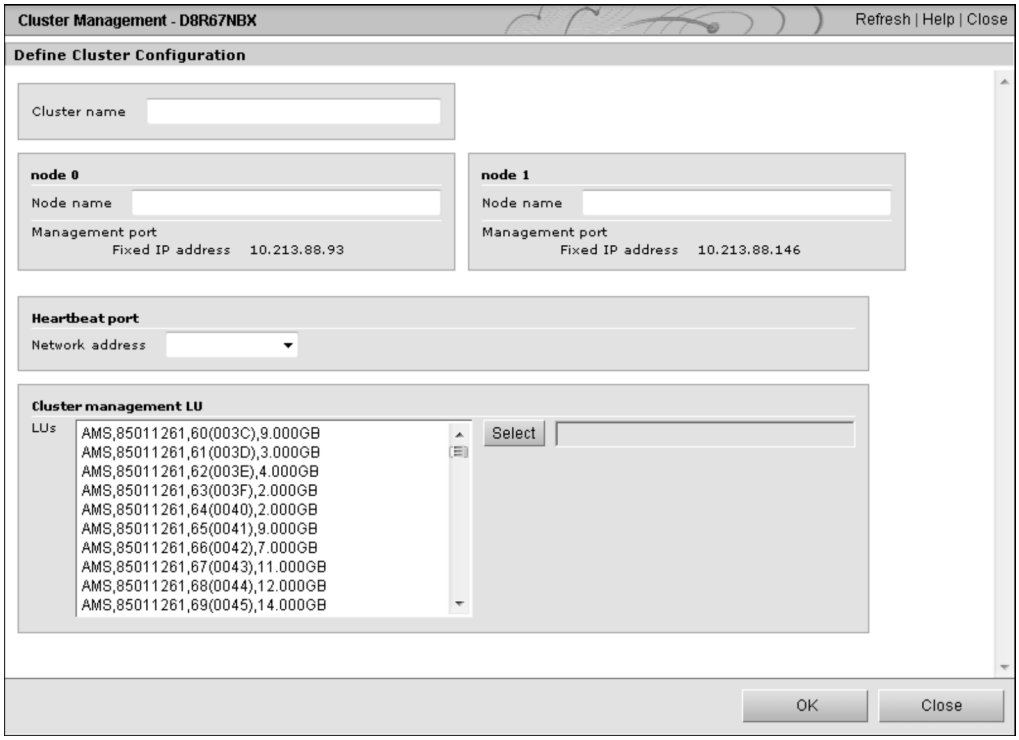


Figure 12.7-1 [Define Cluster Configuration] page

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the "User's Guide" for the version.

(3) Click [OK] button without changing any input contents.

NOTE: If the already input contents are changed, a problem such as unavailable to configure the cluster might be occurred. Do not change the input contents.

Copyright © 2010, 2015, Hitachi, Ltd.

12.8 Recovery of Encryption Key of the HCP Payload Encryption Function

NOTE: If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not necessary because it is performed in the reference guide stated in 12.6.2.

If the system setting information is restored from the system setting information file and the HCP payload encryption function is used, run the hcprecoverkey command to recover the encryption key.

For the reference place of the user`s guide, refer to "General 'Reference Place in User's Guide for Operating Procedures' Table 6 [hcprecoverkey] (GENE 00-0060)".

For the password and the passphrase questioned interactively after running the command, enter the password and the passphrase prepared in Troubleshooting "12.1.6 Prepare the Password and the Passphrase of the HCP Payload Encryption Function" (TRBL 12-0061).

Copyright © 2015, Hitachi, Ltd.

12.9 Start Up the Cluster and the Resource Group

After defining the cluster configuration, start up the cluster and the resource group. However, because the file system recognized by the OS is not on the side of disk array, an error of blocking file system is occurred.

And the resource group becomes the state of an error.

NOTE:
- If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not necessary because it is performed in the reference guide stated in 12.6.2.
- Because the occurrence of errors on the file system and the resource group is the intended result of operation, please go to the next procedure.

12.9.1 Cluster start up

For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Stopping and starting a cluster'' (GENE 00-0040)".

The following shows the procedure to start up the cluster.

(1) Click [Cluster Management] button in [Settings] tab.
[Browse Cluster Status (Cluster / Node Status)] page in [Cluster Management] dialog is displayed. In the state of displaying [Browse Cluster Status (Resource Group Status)] page,
Select [Cluster / Node status] from the drop-down list, then click [Display] button.

(2) Click [Start] button of the cluster.
In the state of stopping the cluster, [Start] button is displayed.
Once [Start] button is clicked, it starts all the nodes that configure the cluster. Once the node is started, it is the state that can starts the resource group.

12.9.2 Start up the resource group

For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Stopping and starting a resource group'' (GENE 00-0040)".

The following shows the procedure to start up the resource group.

(1) Click [Cluster Management] button in [Settings] tab.
[Browse Cluster Status (Cluster / Node Status)] page of [Cluster Management] dialog is displayed.

(2) Select [Resource group status] from the drop-down list, and then click [Display] button. [Browse Cluster Status (Resource Group Status)] page is displayed.

(3) Select the resource group in the radio buttons, and then click [Start] button.
Once [Start] button is clicked, the service that is provided by the selected resource group does not start and the resource group ends abnormally.

NOTE: In the case of not allocating the file system in the node, the state of resource group becomes [Online/No error], but please go to the next procedure.

Copyright © 2010, 2015, Hitachi, Ltd.

12.10 Forcibly Stop the Resource Group

NOTE: If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not required.

Terminate forcibly the resource group which becomes abnormal state at the operation of Troubleshooting “12.9 Start Up the Cluster and the Resource Group” (TRBL 12-0210).

For the reference place in User’s Guide, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 4 ‘Performing a forced stop for a resource group” (GENE 00-0040)”.

The following shows the procedure to terminate the resource group forcibly.

(1) Click [Cluster Management] button in the [Settings] tab.
[Browse Cluster Status (Cluster / Node Status)] page of the [Cluster Management] dialog is displayed.

(2) Select [Resource group status] from the drop-down list, and click [Display] button.
[Browse Cluster Status (Resource Group Status)] page is displayed.

(3) Click [Perform Forced Stop] button of the resource group.
Once [Perform Forced Stop] button is clicked, it ignores all the errors and terminates the resource group forcibly.

NOTE: When the resource group is in the state of [Online/No error], stop the resource group by clicking [Stop] button at the step (3).

Copyright © 2010, 2015, Hitachi, Ltd.

12.11 Record the Result of fslist

NOTE: If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not required.

Execute fslist command to record and store the setting contents of the file system that is created at the node.

Execute fslist command for the both nodes.

For the reference place in User's Guide describing the details about fslist command, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 6 'fslist'' (GENE 00-0060)".

It is based on the premise of registering the public key on the account of SSH. If it is not registered, refer to the "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Registering a public key'' (GENE 00-0050)" for the reference place in User's Guide, and register the public key.

Figure 12.11-1 shows an example of fslist command execution.

Record the information of the file system from the result of fslist command.

Record the parts that are circled in the example of execution at the very least.

```
$ sudo fslist -m –t -p
List of File Systems:
The number of file systems(1)
File system(used by)    : FS1(WORM)
Total disk capacity(GB) : 1.000
Device status           : normal
Device files            : lu14
Block used(GB)          : 0.004
Block free(GB)          : 0.959
I-node used             : 13
I-node free             : 1015795
Volume manager          : use
Mount status            : rw
Quota                   : on
ACL type                : Advanced ACL
Stripes                 : 2
Stripe size(KB)         : 64
Model                   : AMS
Serial number           : 85011261

The number of file systems(2)
File system(used by)    : filesystem02
...
```

Figure 12.11-1 An example of fslist command execution

Copyright © 2010, 2015, Hitachi, Ltd.

12.12 After Deleting the File System, Start the Resource Group and Re-create the File System

NOTE: If you select the collective recovery of the system setting information and the user data for the data recovery method, this procedure is not required.

To restore the blocked file system, once delete the file system and re-create the file system.

The procedure is expressed in the following.

12.12.1 Deleting file system

The following shows the procedure to delete the file system.

For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Deleting a file system'' (GENE 00-0040)".

(1) Execute the HFSM refresh by clicking [Refresh Processing Node] button.
For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Refreshing processing node information'' (GENE 00-0040)".
Although there is a case that an error is output in the pop-up window, the refreshing process is done. Therefore, go to the next step.

(2) Click [Delete File System] button in the state of selecting the check box of the target file system.
[Delete File System] button is displayed in the following sub-window.
- [File Systems] sub-window.
- [File System] sub-tab of [File Systems] in [<Physical Node>] sub-window.

(3) Confirm the information displayed in the confirmation dialog, and then click [Confirm] button by checking the check box.

(4) Confirm the processing result that is output to the pop-up window, and click [Close] button.

12.12.2 Rebooting OS

The following shows the procedure to reboot the OS.

For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Rebooting OS'' (GENE 00-0040)".

(1) Select the check box of the target Processing Node on the [HDI] tab of [Processing Nodes] sub-window, and click [Shutdown Node] button.

(2) Check the information displayed on the confirmation dialog, click [Confirm] button by selecting the check box.

(3) Confirm the result of processing, and click [Close] button.

(4) After confirming the stop of both OSs, select the check box of target Processing Node on the [HDI] tab in the [Processing Nodes] sub-window, and then click [Start Node] button.

(5) Confirm the information displayed in the confirmation dialog, and then click [Confirm] button.

(6) Confirm the processing result that is output to the pop-up window, and click [Close] button.

Copyright © 2010, 2015, Hitachi, Ltd.

12.12.3 Starting resource group

The following shows the procedure to start up the resource group.

For the reference place in User's Guide, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Stopping and starting a resource group'' (GENE 00-0040)".

(1) Click [Cluster Management] button in [Settings] tab.
[Browse Cluster Status (Cluster / Node Status)] page of [Cluster Management] dialog is displayed.

(2) Select [Resource group status] from the drop down list, and click [Display] button. [Browse Cluster Status (Resource Group Status)] page is displayed.

(3) Select a resource group with the radio button, and then click [Start] button.
Clicking [Start] button starts the service provided by the selected resource group.

Copyright © 2010, 2015, Hitachi, Ltd.

12.12.4 Creating file system

Create a file system in accordance with the result of fslist that is obtained at the Troubleshooting “12.11 Record the Result of fslist” (TRBL 12-0230).

The following shows the procedure to create a file system.

For the reference place in User’s Guide describing the details about creating a file system, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 4 ‘Creating a file system” (GENE 00-0040)”.

(1) Click [Create File System] button.
[Create File System] button is displayed on [File System] sub-tab of [File Systems] in the [<Physical Node>] sub-window.

(2) Specify the necessary information from [Create File System] dialog.
Specify the basic attribute that is related to the file system on [Basic] tab.

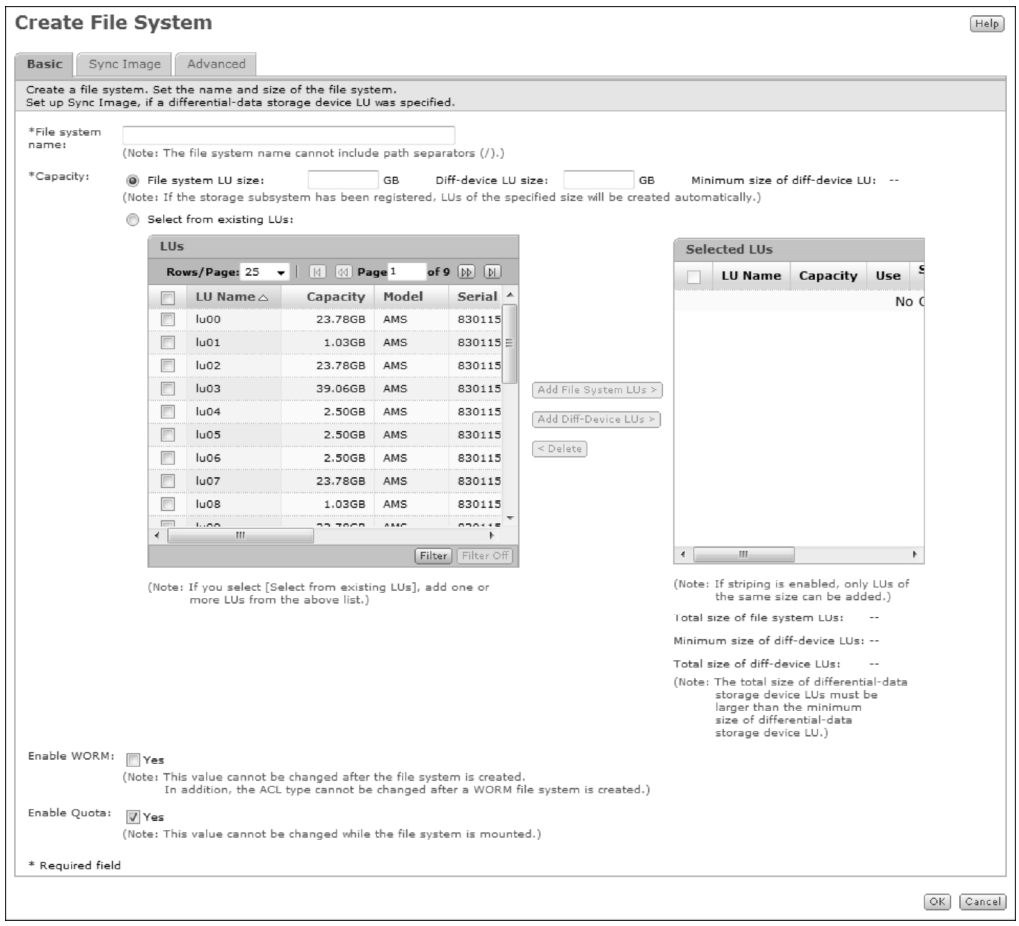


Figure 12.12.4-1 [Basic] tab on [Create File System] dialog

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the “User’s Guide” for the version.

(3) Specify the necessary information, and then click [OK] button.

(4) Check the information displayed on the confirmation dialog, and then click [Confirm] button.

(5) Check the result of processing that is output from the pop-up window, and then click [Close] button.

Copyright © 2010, 2015, Hitachi, Ltd.

12.13 Execute the Restoration of Data in the File System

12.13.1 arcrestore command execution

Restore the data that has been stored in the file system by using arcrestore command.

Figure 12.13.1-1 shows an example of arcrestore command.

For the reference place in User's Guide describing the details about arcrestore command, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 6 'arcrestore" (GENE 00-0060)".

- The target file system to be restored is "fs01".
- The name of the name space that is set to the file system to be restored is "fs01namespace".

The value which is input here uses the combination of the file name which is recorded at Troubleshooting "12.1.5 Record the name space name of the HCP to be connected" (TRBL 12-0060) and the name space name.

```
# sudo arcrestore --file-system fs01 --namespace 'fs01namespace'
KAQM37077-Q Do you want to restore the file? (y/n)
```

Figure 12.13.1-1 An example of arcrestore command execution

NOTE: If you want to restore the file again, in such a case because it mistook the combination of name space name between the file system and the name space to be restored, execute in reference to Troubleshooting "12.12 After Deleting the File System, Start the Resource Group and Re-create the File System" (TRBL 12-0240) without deleting the data in the file system.

Copyright © 2010, 2015, Hitachi, Ltd.

12.13.2 Consistency check of the file that restored

NOTE: Although hcporphanrestore command may take much time to complete, you can execute the procedure of Troubleshooting “12.14 Set the Sharing by Using the Information Recorded in Advance” (TRBL 12-0290) without waiting the completion after executing the command.

Use hcporphanrestore command, and execute the procedure to check whether there is no inconsistency in the restored file.

Figure 12.13.2-2 shows an example of hcporphanrestore command.

For the reference place in User’s Guide describing the details about hcporphanrestore command, refer to “General ‘Reference Place in User's Guide for Operating Procedures Table 6 ‘hcporphanrestore” (GENE 00-0060)”.

- The file system to be executed the consistency check is “fs01”.

```
# sudo hcporphanrestore --file-system fs01
Duplication
/rest/ccc/dd/cccdd00
/mnt/fs01/dir2/file2-13-2 85

Duplication
/rest/ccc/dd/cccdd01
/mnt/fs01/dir2/file2-3

Orphan
/rest/aaa/bb/aaabb00
/mnt/fs01/dir1/file1-1

Orphan
/rest/aaa/bb/aaabb01
/mnt/fs01/dir1/file1-2
```

Figure 12.13.2-2 An example of hcporphanrestore command execution

Copyright © 2010, 2015, Hitachi, Ltd.

12.14 Set the Sharing by Using the Information Recorded in Advance

12.14.1 Set the Sharing by Using the recorded file

Set the common information of the file system by using the information recorded at Troubleshooting "12.1.4 Record the shared setting of file system" (TRBL 12-0040).

Set the sharing in the file system with cifsrestore/nfsrestore command by using the information definition file that is obtained at the cifsbackup/nfsbackup.

Figure 12.14.1-1 an example of cifsrestore command execution shows an example when the information of CIFS sharing is restored.

- The name of the file system is fs01.
- Information definition file name is fs01_cifsshares.xml.

```
$ sudo cifsrestore fs01_cifsshares.xml
```

Figure 12.14.1-1 An example of cifsrestore command execution

Figure 12.14.1-2 an example of nfsrestore command execution shows and example when the information of NFS sharing is restored.

- The name of the file system is fs01.
- Information definition file name is fs01_nfsshares.xml.

```
$ sudo cifsrestore fs01_cifsshares.xml
```

Figure 12.14.1-2 An example of nfsrestore command execution

Copyright © 2010, 2015, Hitachi, Ltd.

12.14.2 Set the sharing by using information that is manually recorded

If you set the sharing by using information that is manually recorded, without using information definition file that is obtained at cifsbackup/nfsbackup. You can use the information of table from "Table 12.1.4-1(TRBL 12-0040) to Table 12.1.4-6 (TRBL 12-0050)".
The following shows the overview of procedure to create the sharing manually.

For the reference place in User's Guide describing the details about setting a sharing, refer to "General 'Reference Place in User's Guide for Operating Procedures Table 4 'Adding a file share" (GENE 00-0050)".

(1) Click [Add Share] button.
[Add Share] button is displayed in the next sub-window.

- [<file system>] sub-window

(2) [File System] sub-tab of [File Systems] in the [<Physical Node>] sub-window.
Specify the necessary information at the [Add Share] dialog.
At [Basic] tab, specify the basic attribute that is related to file sharing.
At [Access Control] tab, specify the attribute that is related to access right of the file sharing.

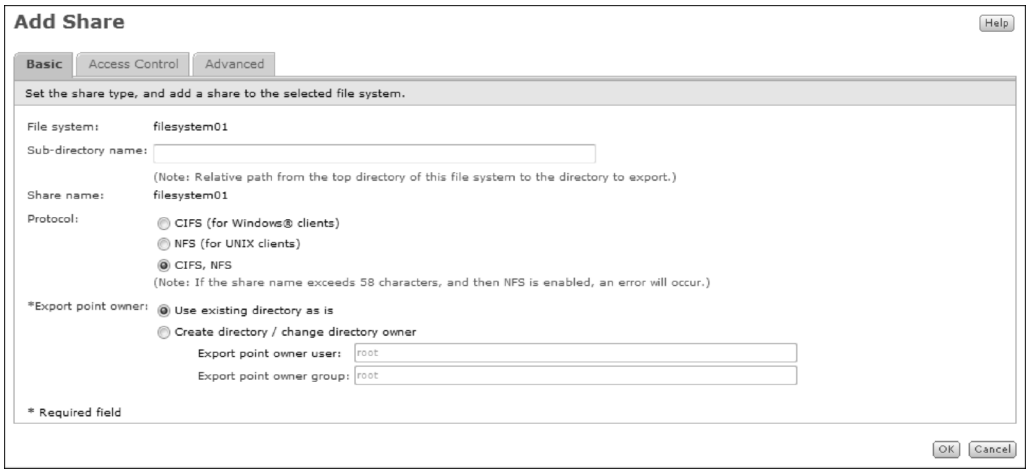


Figure 12.14.2-1 [Basic] tab of [Add Share] dialog

NOTE: The contents of the window may be changed depending on the version. For the details, refer to the "User's Guide" for the version.

(3) After specifying the necessary information, click [OK] button.

(4) Check the information displayed in the confirmation dialog, then click [Confirm] button.

(5) Confirm the result of the processing which is output to the pop-up window, then click [Close] button.

Copyright © 2010, 2015, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, Hitachi, Ltd.